Federal Ministry
of the Interior

# Protecting Critical Infrastructures – Risk and Crisis Management

## A guide for companies and government authorities

www.bmi.bund.de

# Foreword

Our society's existence depends on securing the supply of a wide variety of products, services and functions. Protecting vital institutions is therefore a key responsibility of state security. The threat of international terrorism and the increasing number of natural disasters pose a growing challenge for the protection of such critical infrastructures. And information technology, which has pervaded all areas of life and economic activity, brings new vulnerabilities. Because most of the infrastructures which are critical for our society are privately operated, in Germany the government and the private sector work hand in hand to ensure effective protection for these systems and facilities. The security authorities assist the private companies with advising and networking as well as specific recommendations for action. And the private sector contributes its expertise and practical experience to this partnership.

This guide to risk and crisis management is one product of such cooperation. The guide is addressed to operators of critical infrastructures and is intended to help them create and expand their own systems of risk and crisis management. Drawing on the general recommendations in the Baseline Security Strategy for the Protection of Critical Infrastructures (Federal Ministry of the Interior, 2005), this guide offers methods for implementing risk and crisis management and practical tools in the form of examples and checklists. When developing this guide, the Federal Ministry of the Interior, the Federal Office of Civil Protection and Disaster Assistance and the Federal Office for Information Security received assistance from experts with practical experience in the private sector. The Federal Ministry of the Interior would therefore like to thank the following for their help throughout the entire process:

- the employers' liability insurance association for banks, insurance companies, administrations, liberal professions and special companies, Mr Bernd Marquardt and Mr Hans-Jürgen Penz;
- Commerzbank AG, Mr Heinz-Peter Geil;
- the Forschungszentrum Jülich GmbH, Ms Sonja Altstetter;
- Fraport AG, Mr Friedhelm Jungbluth and Mr Jens Sanner;
- Gelsenwasser AG, Mr Uwe Marquardt;
- Infraprotect GmbH, Mr Wolfgang Czerni;
- Trauboth Risk Management GmbH, Mr Frank Tesch;
- VERISMO GmbH, Dr Klaus Bockslaff;

and their employees.

The following partners also deserve thanks for contributing advice and suggestions: EnBW Regional AG, the German Insurance Association (reg'd. society) and the Arbeitsgemeinschaft für Sicherheit der Wirtschaft e. V. Following the CIP Implementation Plan adopted by the Federal Cabinet in summer 2007 as part of the National Plan for Information Infrastructure Protection, this guide to risk and crisis management is a further contribution by the Federal Ministry of the Interior to strengthen the protection of critical infrastructures. At the same time, it underscores the importance of constructive cooperation between government and the private sector in this key area of internal security.

Berlin, January 2008

# Table of Contents

## Annex

# Summary

This guide offers a management strategy to help operators of critical infrastructures, i.e. companies and government authorities, identify risks, implement preventive measures and deal with crises effectively and efficiently. Critical infrastructures are understood here as organizations and institutions of central importance for the country and its people whose failure or functional impairment would lead to severe supply bottlenecks, significant disruption of public security or other dramatic consequences.

Recent history has shown that infrastructures can indeed be damaged and that disruption of critical processes can have far-reaching social and economic impacts.

Serious damage may be caused by

- natural events,
- technical failure or human error,
- intentional acts of a terrorist or other criminal nature
- and war.

Operators of critical infrastructures need to be aware of these causes and prepare for them. This means identifying and reducing risks as far in advance as possible and preparing for unavoidable crises as much as possible. Doing so helps ensure survival in the event of a crisis, thereby helping companies add value and comply with legal requirements and helping government authorities fulfil their mission of providing vital services.

The strategy for risk and crisis management presented in this guide consists of five phases: planning to set up a system of risk and crisis management, describing the basic aspects of risk analysis, implementing preventive measures, portraying aspects of robust crisis management and evaluating the system of risk and crisis management in an organization. The term “organization” refers here to companies or government authorities which operate critical infrastructures as defined above.

### Phase 1 – Planning in the organization

Thorough planning creates the necessary conditions for successfully implementing all or part of this guide.

Before implementing the guide, fundamental issues need to be clarified, including how risk and crisis management is anchored in the organization, the definition of responsibilities for implementation, availability of resources, clarification of legal obligations to establish risk and crisis management, and the definition of strategic protection aims to be achieved in the company or government authority.

### Phase 2 – Risk analysis

A risk analysis provides a structured overview of an organization’s individual processes, possible threats to these processes and the vulnerability inherent in these processes. Combining this information yields a risk analysis for all critical processes in individual scenarios.

The information on risks can be compared, to provide an easy-to-understand picture of risks in which risk priorities can be identified.

The results of the risk analysis can be evaluated by checking them against the strategic protection aims already set. If it is not possible to achieve most of the strategic protection aims, then concrete measures must be taken to reduce existing risks and make it easier to deal with crises.

### Phase 3 – Preventive measures and strategies

Preventive measures help reduce risks to processes and thus to the provision of products and services. They make organizations more crisis-resistant, helping to reduce the number and intensity of crisis events. Preventive measures are aimed at actively protecting components within organizations or creating redundancies.

Other possibilities include avoiding, shifting or consciously accepting risks. Here, one should be aware that risk avoidance usually entails a certain lack of flexibility for the company or government authority. Shifting risk does not reduce physical risks, but only ensures financial compensation, although this may be significantly less than actual damage caused in individual cases.

### Phase 4 – Crisis management

If a company or government authority experiences serious damage despite preventive measures, crisis management should provide for special structures to deal with the situation.

Crisis management includes special structures and procedures which differ from those for regular operations. During a crisis, decision-making authority is centralized in order to be able to react to situations without delay, containing the impact of a crisis and reducing the time needed to restore normal operations.

### Phase 5 – Evaluation of risk and crisis management

Evaluation covers all phases of risk and crisis management, from the measures identified during planning to checking that risk profiles are current and preventive measures and crisis management are effective. Such evaluation should be undertaken regularly.

Additional evaluations may be necessary

- after measures are implemented,
- after the organization is expanded or restructured, and
- if the threat situation changes.

The annex to this guide contains an example for carrying out a risk analysis and checklists for measures implemented in the organization.

**Contact:**
Bundesamt für Bevölkerungsschutz und Katastrophenhilfe
Abteilung II
Notfallvorsorge, Kritische Infrastrukturen
Provinzialstraße 93
53127 Bonn, Germany
http://www.bbk.bund.de

# 1 Introduction

Infrastructures are an essential part of our highly developed society. In our daily lives, we all rely on infrastructures and depend on their unlimited availability.

Since 1997, the federal government has focused on protecting what are known as critical infrastructures in order to analyse the need for additional protective measures. Critical infrastructures are understood as "organizations and institutions of central importance for the country and its people whose failure or functional impairment would lead to severe supply bottlenecks, significant disruption of public security or other dramatic consequences."[1]

Their constant availability is threatened by natural events, technical failure or human error and intentional acts of a terrorist or other criminal nature. An armed conflict in Germany would also result in enormous damage to infrastructures.

The threat situation has changed constantly over the past years. There are indications that the threat of natural disasters as well as threats posed by terrorist or criminal activity are on the rise, creating new challenges for society.

Like the threat situation, the vulnerability of infrastructures is also changing. Most infrastructure systems today are linked in some way. Disruptions in one area can multiply in other locations, branches or sectors, with an impact that extends far beyond the original area of damage.

The financial and personnel resources available to operators to protect their infrastructure systems are limited, so it is especially important to use these resources efficiently and effectively. To do so, it is essential to be aware of the threats and risks and of the possibility to compare and assess risks in order to set priorities. This then provides the groundwork for implementing targeted protection measures.

This guide, "Critical Infrastructure Protection: Risk and Crisis Management" is the product of collaboration among private industry, government authorities and a research institute. The guide applies to all sectors and is intended for companies and government authorities as a tool for self-analysis.

It brings together information on the theory behind risk and crisis management with practical checklists and an example of risk analysis with the aim of enabling companies and government authorities to set up or expand an effective and efficient system of risk and crisis management on their own or with external help.

From the federal perspective, the overarching goal is to reduce the impact of extreme incidents on critical infrastructures and to be better able to handle anticipated crises.

[1] As defined by the Working Group on Infrastructure Protection (AK KRITIS) at the Federal Ministry of the Interior on 17 November 2003.

2

# Basic information about critical infrastructures

## 2.1 Sectors

Critical infrastructures as defined in the Introduction are mainly found in the following sectors:

- energy (electricity, oil, natural gas)
- water and food supply, health care, emergency medical services
- information and communications technology
- transport
- hazardous materials (chemical industry and biological substances)
- banking and finance
- government authorities, public administration and the judicial system
- media, major research institutes and cultural assets

## 2.2 Critical infrastructures: Framework conditions and characteristics

In recent years, disruptions of critical infrastructures have repeatedly been characterized by two features:

1. Widespread impact on infrastructures caused in particular by natural threats, with regional, national or Europe-wide impacts (e. g. flooding of the River Elbe in 2002, winter storm Kyrill in 2007).

2. Local disruptions or damage have impacts which in some cases extend far beyond the original area of damage due to networks and connections across regions and between systems (e. g. shutdown of a power line across the River Ems in 2006 which led to blackouts in parts of Europe).

In the following, the central elements of changed and changing framework conditions and characteristics are analysed, providing the basis for developing a system of risk and crisis management using this guide.

### 2.2.1 Changes in the threat situation

Disruptions to critical processes of infrastructure systems can have far-reaching social and economic consequences. Although the following examples do not clearly indicate a trend towards a more critical threat situation, they do confirm the need for ongoing protection of critical infrastructures.

**Example: Extreme weather**
Extreme weather can have a direct impact on infrastructure systems. It is still too early to reliably predict changes in extreme weather events in Germany due to global climate change, as there is not yet enough information on atmospheric warming and its effects on Germany. However, some trends, such as an increase in heavy precipitation, have shown up in weather data. Flooding on the rivers Oder in 1997 and Elbe in 2002 and around the Alps in 2005 follows this pattern.[2]

**Example: Public health threats (influenza pandemic)**
In the 20th century, there were several major outbreaks of influenza, including the Spanish flu pandemic in 1918 which killed more than 50 million people world-wide. Today, experts agree that it is only a matter of time until a new and highly dangerous virus evolves from mutations. An influenza pandemic would also spread throughout Germany via the country's international transport hubs. The effects would threaten all areas of life, including the entire private sector and government agencies. Not only can a pandemic affect demand for products and services, it can also threaten the entire economic and social infrastructure. The availability of many resources and services could be limited or cut off entirely. Due to mutual dependencies, this can lead to a domino effect shutting down much of the government, economy and society.[3] Models calculated for Germany figure an infection rate of 15–50 percent.[4] In addition to employees who are unable to work because they are ill, others would stay home to care for sick family members or out of fear of infection, significantly increasing the absentee rate.

[2] Rahmstorf et al., 2006, p. 70.

[3] Federal Office for Civil Protection and Disaster Assistance, 2007.

[4] Robert Koch Institut 2007b, p. 4.

**Example: International terrorism**
International terrorism is characterized by loosely structured networks. Individual cells are connected by little more than common aims; they operate largely independent of each other and without a central command structure. Such loose networks are able to act quickly and flexibly without being detected.[5] In 2006, attempts to set off bombs on two regional trains failed for technical reasons; in 2007, the authorities were able to prevent planned attacks against a number of US installations in Germany.

**Example: Information technology**
The news media report almost daily on hacker attacks or industrial or economic espionage. Even apart from such threats, however, hard- and software failures and simple human error can lead to significant impacts and damage to critical infrastructures. One example is the large-scale power outages in the US and Canada in 2003 largely due to problems with one electricity provider's transmission system. Another example is the collapse of the entire EC debit card system in Switzerland in 2000 resulting from an error in one computing centre.

### 2.2.2 Socio-economic framework conditions

**Growing dependence**
Private industry and government agencies increasingly depend on external providers of goods and services. One such service, the supply of electricity, is extremely important. Almost every single service depends directly or indirectly on the reliable supply of electricity.

**Subjective perceptions of risk**
Government and private industry invest a great deal of money in security and count on this investment being effective. However, the positive effects of security measures are often not measurable in objective terms. Instead, companies or government authorities regard long periods without crises as confirming the effectiveness of measures taken, which can lead them to overlook potential threats and vulnerable areas.

And in practice, the risks identified are often those which appear to be manageable or controllable and part of an obvious chain of cause and effect.[6] Other risks are ignored, consciously or unconsciously, and their possible impacts not taken into account when implementing preventive measures.

**Demographic change**
Changes in the age structure of society and migration-related changes to population density within Germany create new demands on critical infrastructures, in some cases with ramifications for security. For example, decreasing water consumption and the resulting reduced flow of water to end users can create hygiene problems in water supply systems.

**Changed economic framework conditions**[7]
Changes in market activity, such as those caused by market liberalization and privatization of state-owned infrastructure operators, can affect the level of security and investment in security measures. Competition and the pressure to cut costs create conditions in which security precautions such as back-up systems and other buffers are reduced. Although operators largely comply with regulatory requirements, increasingly precise calculations allow them to take greater advantage of room for discretion and to reduce security buffers, which are then missing especially in crisis situations.

### 2.2.3 Special characteristics of critical infrastructures

**Networks within sectors**
Infrastructure services are provided over large areas via physical, virtual or logical networks. These networks are growing in size and complexity. Intersections within these networks represent possible areas of vulnerability, where disruption can lead to regional, interregional, national or even global outages or failures. Information and communications technology and the supply of electricity, water and natural gas in particular rely on networks of this kind.

**Links between sectors (interdependence)**
Infrastructure systems are characterized by a high degree of interconnection. Thanks to the rapid spread of information technology, this development has gained momentum over the past 15 years. In addition to making supply processes more efficient, such interconnection also creates interdependencies which in many cases can be measured only in qualitative terms. Many physical, virtual and logical dependencies are not apparent until a crisis occurs and the connection breaks down. The high level of interdependence can lead to cascading shut-downs.[8] At the same time, smaller and smaller disruptions are enough to cause dramatic consequences in complex systems (vulnerability paradox).[9]

[5] Cf. Lewis 2006, p. 1.

[6] Dost 2006.

[7] Cf. International Risk Governance Council 2006, pp. 11–17.

[8] Cf. Lewis 2006, p. 57.

[9] Rosenthal 1992, p. 74 f.

Figure 1 "Interdependencies of selected critical infrastructures" shows the interdependencies between selected critical infrastructures. Here, only direct dependencies between individual sectors or branches are initially taken into account.

**Changed technological framework conditions**
Technology, especially information technology, is developing at a rapid pace. Often, new developments can be introduced only in certain areas, leaving old components and procedures in place alongside new ones. New hard- and software that has been introduced without sufficient testing or with errors; incompatible systems; inadequately planned migrations to new hard- or software platforms; and staff not properly trained to use the new components can all lead to security gaps and areas of weakness which could, under certain circumstances, cause the entire system to fail.

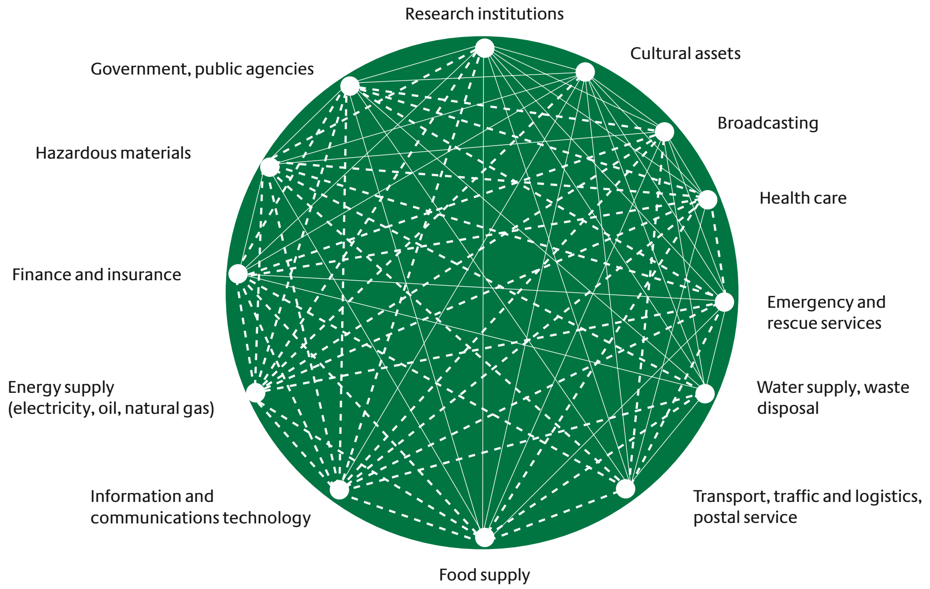
**Types of damage**
Critical infrastructures are subject to many different types of damage, from actual physical harm or damage to persons or property, to financial losses, psychic harm and anxiety, to the public's loss of faith in the political leadership.

## 2.3 Legal requirements concerning risk and crisis management

Public limited companies and limited liability companies (GmbH) are currently subject to overarching legal requirements for controlling risk and crises. The financial sector also has regulations which are obligatory in practice, such as minimum requirements for risk management (MaRisk). According to these regulations, the concept of enterprise security includes protecting persons and material goods such as buildings and facilities, maintaining operations through any kind of disruption up to a crisis, whether a stock market crisis, natural disaster or terrorist attack.

The Trading (Control and Transparency) Act (KonTraG) adds to the Stock Corporation Act the obligation to set up a monitoring system for the purpose of enterprise risk management. The regulation refers only to public limited companies, but in practice applies also to partnerships limited by shares (KGaA) and large limited liability companies (GmbH), in particular those with codetermined or optional supervisory boards.

**Figure 1: Interdependencies of selected critical infrastructures**


Research institutions
Cultural assets
Broadcasting
Health care
Emergency and rescue services
Water supply, waste disposal
Transport, traffic and logistics, postal service
Food supply
Information and communications technology
Energy supply (electricity, oil, natural gas)
Finance and insurance
Hazardous materials
Government, public agencies

Market risks are often dealt with in the context of the Trading (Control and Transparency) Act. By contrast, security risks[10] and risks from events of nature are often underestimated, although the Act covers all risks that could threaten an enterprise's existence. Section 91 (2) of the Stock Corporation Act (AktG), for example, obliges the management boards and auditors of annual accounts of public limited companies "to take appropriate measures, in particular to set up monitoring systems, in order to identify at an early juncture developments which threaten the company's existence." However, the law does not indicate any method to serve as a standard. Thus the specific measures are left up to the individual enterprises. The internal monitoring system should be designed to identify threatening developments early enough so that appropriate measures can be taken to safeguard the company's existence.

Thus the company's management has a legal obligation to implement an effective system of risk management. If it fails to do so, the auditor may refuse to certify the company's annual accounts. The auditor is thus responsible for checking whether the board has provided for appropriate risk management (Section 317 (4) Commercial Code). This includes an assessment of threats, evaluations of any interruptions of operations, implementation of systematic measures to avoid such interruptions, and a regularly updated emergency plan.[11] Setting up a monitoring system is one of a board's general obligations under Section 76 (1) of the Stock Corporation Act. In case of damage, the board can be held liable under Section 93 (2) of the Act if the board has violated its duty to take due care.

Not only the Trading (Control and Transparency) Act, but also the harmonized European insurance law Solvency II requires risk management for enterprises which takes into account all risks which may confront insurers. By including possible risks in the terms of insurance, the insurer can make the provision of insurance protection conditional on preventive measures taken and thus implicitly on a system of risk management. Under Section 6 (1) of the Act on Insurance Contracts (VVG), failure to fulfil the terms of insurance leads to loss of cover.

In the same way, the Basel II Capital Accord, which is intended to minimize the effects of bank failures, explicitly requires that banks' operational risks be taken into account along with market and credit risks. Even though Basel II only deals with risks to financial institutions, it is possible that banks will in turn require enterprises to account for their risks, thereby making lending conditional on risk management. If the system of risk management sufficiently considers and accounts for all risks, this can result in more favourable lending terms, as it reduces the bank's risk of failure.

[10] See: Federal Ministry of the Interior 2005.

[11] Cf. Bockslaff 1999, p. 109.

# 3 Risk and crisis management

## to protect critical infrastructures

The strategy for risk and crisis management presented in this guide constitutes a systematic process and consists of five phases representing the necessary scope of process-based risk and crisis management in a private enterprise or a government authority. The five phases are as follows: 1. preliminary planning to establish a system of risk and crisis management; 2. risk analysis; 3. specification of preventive measures; 4. implementation of a system of crisis management; and 5. regular evaluation of phases 1 through 4. The figure 2 "The five phases of risk and crisis management" illustrates this strategy and shows the process in the form of a chart.

As described here, risk and crisis management is based on a general "plan – do – check – act" (PDCA) management cycle. This allows it to be incorporated into existing management structures such as quality management, existing risk and crisis management, or process management. The term "organization" refers here to private enterprises or government authorities which operate critical infrastructures as defined above.

Figure 2: The five phases of risk and crisis management[12]

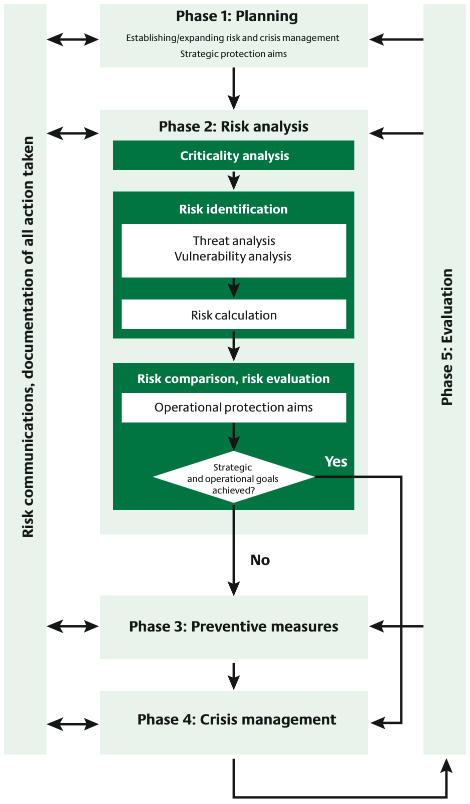
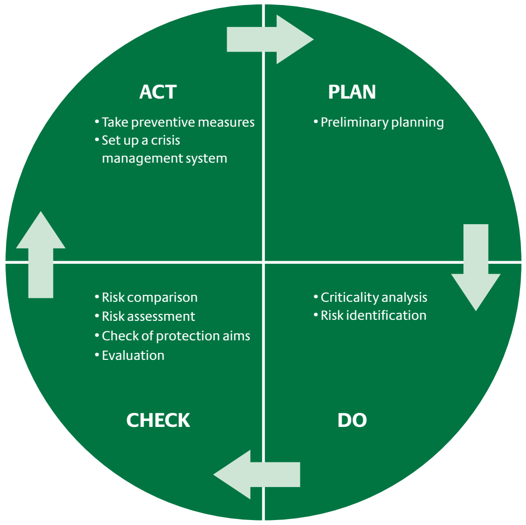

Phase 1: Planning
Establishing/expanding risk and crisis management
Strategic protection aims
Phase 2: Risk analysis
Criticality analysis
Risk identification
Threat analysis
Vulnerability analysis
Risk calculation
Risk comparison, risk evaluation
Operational protection aims
Strategic and operational goals achieved?
Yes
No
Phase 3: Preventive measures
Phase 4: Crisis management
Risk communications, documentation of all action taken
Phase 5: Evaluation

Figure 3: The process of risk and crisis management based on PDCA[13]



[12] Cf. Australian/New Zealand Standard 2004, p. 13; Trauboth 2002, p. 23.

[13] Cf. Gesellschaft für Anlagen- und Reaktionssicherheit 2007, p. 21.

## 3.1 Phase 1: Preliminary planning

Thorough preliminary planning creates the necessary conditions for successfully establishing risk and crisis management in a private enterprise or a government authority.

Before applying this guide, fundamental issues need to be clarified, in particular how the organization's leadership establishes risk and crisis management; acceptance of the process; definition of responsibilities; availability of resources and definition of strategic protection aims.

### 3.1.1 Establishing risk and crisis management

Creating or expanding a system of risk and crisis management is initiated by the organization leadership, which also clarifies the goals it intends to pursue. The system is implemented and applied at the working level, and staff are involved in the process.

Creating risk awareness throughout the entire organization by means of consistent and transparent risk policy must receive special attention, because the quality of risk management depends on staff acceptance and motivation.

### 3.1.2 Division of responsibilities

The process of establishing risk and crisis management should be led by someone with expertise in this field, who is also responsible for overseeing the substantive aspects of the project. The project leader should consult with the head of the organization as needed. It is advisable to assign this task to the manager responsible for this area in the enterprise or government authority.

The head of the organization is responsible for making basic decisions arising from the creation or expansion of risk and crisis management. This applies in particular to approval of financial and staff resources.

It is difficult to know ahead of time which tasks will need to be assigned in the course of implementing risk and crisis management. These can be specified during implementation.

### 3.1.3 Resources

The needs arising from establishing risk and crisis management are estimated in advance. If necessary, an interdisciplinary task force made up of organization staff can be set up to provide support to the project leader and take over individual tasks. It helps if these staff have a detailed understanding of the organization's structure. All the main divisions of the organization should be represented on the task force.

If the necessary expertise in risk and crisis management is lacking within the organization, staff may be given additional training or outside specialists may be hired.

The resources needed to apply risk and crisis management within the organization will be identified during the course of the project.

### 3.1.4 Clarifying legal obligations

Preliminary planning includes clarifying legal obligations to establish a system of risk and crisis management.

### 3.1.5 Strategic protection aims

When establishing risk and crisis management, strategic protection aims need to be formulated to define what the system of risk and crisis management is intended to achieve.

Protection aims are heavily influenced by ethical, operational, technical, financial, legal, social and environmental aspects.[14][15] They display the following characteristics:

- they describe the status quo,
- they create room to implement various measures, and
- they are specific, measurable, accepted, realistic and time-dependent (SMART).

Examples:

- best possible protection of staff and others on site (e. g. clients),
- maintenance of the organization's functionality even in extreme situations,
- compliance with legal requirements,
- prevention of major economic damage, and
- prevention of possible damage to the organization's image.

[14] Examples: human life, social relevance of the product or service provided, size of the facility, financial resources, guidelines, regulations.

[15] Australian/New Zealand Standard 2004, p. 15.

### 3.1.6 Risk communications

In general, risk communications refer to “all communication processes related to identifying, analysing, assessing and managing risks and the necessary interactions between those involved.”[16] Risk communications provide the platform for risk awareness and risk acceptance in private enterprises and government authorities. Both aspects are essential for successful risk management. In the present context, it is useful to distinguish between an organization’s internal and external risk communications.

Internal risk communications refer to all communicative interaction concerning risk within an organization: from establishing the system of risk management to evaluating it. Risk communications should be given special attention during the process of establishing a system of risk management. It is crucial to discuss the subject and aims of risk management at an early stage with those who will be responsible for it. Successful internal risk communications are the prerequisite for successful external risk communication.

External risk communications are not aimed merely at informing and instructing the media and those affected; rather, they seek a dialogue tailored to a specific audience. Here one must always remember to communicate risk-related topics in such a way that no misunderstandings can arise between sender and receiver. For example, empirical research has demonstrated differences in the way experts and ordinary persons perceive risk. In order to avoid unacceptable results, risk communications should always be timely, unambiguous, audience-appropriate, consistent and reliable. For risk communications to be effective, the audience must trust the source and find it credible.[17]

## 3.2 Phase 2: Risk analysis

A risk analysis structures and objectifies the information gathered on threats and risks in private enterprises and government authorities. In this guide, risks refer to processes and their individual components. Risk analysis studies different processes and their components and compares their different risks for the organization. This comparison makes it possible to determine the urgency and priority of measures that can have a significant influence on risk. In this way, risk analysis provides the basis for managing limited financial and personnel resources effectively and efficiently.

As understood in this guide, risk analysis should answer the following questions:

- What kind of threats may arise?
- How likely are these threats to arise where the organization is located?
- Which areas would be vulnerable in case of threat?

These questions show that the analysis of risks inherent in processes or their components addresses information about threats and about the vulnerability of processes and their components.

This guide deals with operational processes, i.e. core and supporting processes, which will not be treated separately in the following and thus are referred to as processes or sub-processes; in this guide, sub-processes are understood as individual segments of processes.

The risk analysis starts by dividing the organization into processes and sub-processes. The organization itself decides the degree to which sub-processes are further subdivided; for example, if a control room is identified as part of a process, it can be defined as a sub-process. It is also possible to divide the control room itself into further sub-processes. The more levels of sub-processes there are, the more effort a risk analysis will require; however, it will also have greater informational value.[18]

[16] Jungermann et al., 1991, p. 5.

[17] For more information on detailed planning of risk communication, see Wiedemann et al. 2000 and Gray et al. 2000.

[18] For more information on processes and their representation, see Gesellschaft für Anlagen- und Reaktorsicherheit 2007.

**Figure 4: Process, sub-processes, risk elements**

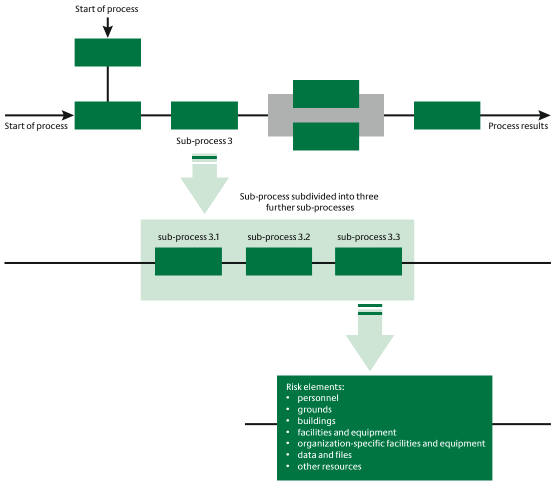


Figure 4 "Process, sub-processes, risk elements" provides a schematic representation of a process, its sub-processes and their division into further sub-processes and their components.

Components of sub-processes are those elements that contribute to the function of a process. These elements are called "risk elements" in this guide. They are individual physical or virtual elements which may be harmed or damaged, with an impact on the sub-process in question. This guide covers the following risk elements:

- People (staff and others on the premises):
  It is essential to protect everyone on the premises sufficiently against threats or to take them to safety in case of imminent threat. To do so, all organizations must take precautions to provide the best possible protection for those on site, especially before police, fire and emergency service personnel arrive in the event of an emergency and after they leave.

  Staff, in particular specialized staff, are risk elements in the sense of retaining functionality of sub-processes.

- Grounds:
  This includes all outdoor areas, including roads, storage and parking areas, green spaces and areas essential to operations.

- Buildings:
  These include all structures above and below ground, such as production halls, warehouses and administrative buildings as well as parking garages.

- Facilities and equipment:
  Facilities and equipment of sub-processes can be found in all areas of an organization, particularly in the following:

  - electricity supply,
  - natural gas supply,
  - district heating,
  - water supply,
  - information technology (IT),
  - communications technology (CT) and
  - transport (including vehicles and fuel supply).

- Special, organization-specific facilities and equipment:
  This includes all specialized facilities and equipment.[19]

**IMPORTANT NOTE:**
Identifying the relevant organization-specific risk elements is one of the most important prerequisites for a successful risk analysis, since critical processes are often directly dependent on organization-specific facilities and equipment.

- Data and files:
  These include all information kept in electronic and paper form needed to maintain sub-processes in the organization.

- Other resources:
  As referred to in this guide, this covers all other means of production not already mentioned.

### 3.2.1 Criticality analysis

A criticality analysis allows an organization to identify which processes out of all those listed would have far-reaching consequences for the organization if disrupted. Appropriate measures must be taken to protect such critical processes sufficiently. The identification of risks and, above all, the preventive measures chosen to reduce risk should initially concentrate on risk elements of the sub-processes of critical processes.

[19] Examples: Control components, software, medical equipment, special heating and ventilation systems, secure entry systems, storage tanks, aircraft.

The following criteria may be used to identify critical processes:[20]

- Life and health:
  If the process is disrupted, what will be the impacts on human life and health?

- Time frame:
  If the process is disrupted, how long will it take to have an impact on the organization's overall product/service? The shorter the time, the more critical the process.

- Magnitude:
  How much of the overall product/service will be affected if this process is interrupted or completely stopped?

- Contractual, regulatory or legal relevance:
  If the process is disrupted, what contractual, regulatory or legal consequences will this have for the organization?

- Economic damage:
  If the process is disrupted, what is the estimated financial damage to the organization?

The organization should decide which criteria to use, how many criteria should apply at once and what classification to use within the criteria.

The criticality analysis results in identifying all critical processes in an organization and portraying the sub-processes at work in them as well as their risk elements.

### 3.2.2 Risk identification

An organization's risks are determined by the threats arising at its location(s) which may impact on its risk elements and by the vulnerability of these risk elements. Combining the relevant information on threats and vulnerability results in identifying the risk to the risk elements in question and, when aggregated, to the sub-processes in question. In this guide, risks to the risk elements are called sub-risks; aggregated risks to the sub-processes are called overall risks. The aspects of risk identification are described in detail in the following sections.

#### 3.2.2.1 Threat analysis and scenario development

Recognizing and documenting all relevant threats is crucial to a successful risk analysis. The first step in analysing threats and developing scenarios should therefore be drawing up a list of threats that may arise at the organization's location(s). This comprehensive list should describe the general nature of these threats, their intensity, duration and possible effects.[21]

On the basis of a site-specific list of threats, it is possible to develop scenarios containing additional information needed for risk analysis and crisis management. These scenarios should represent realistic incidents that could result in crises. The staff member in charge of risk and crisis management should determine the number of scenarios to be included in the risk analysis. The aim is to cover all possible threats.

The following additional information is gathered for each scenario:

- Anticipated exposure:
  Which sub-processes and risk elements could be affected?

**IMPORTANT NOTE:**
Whether a process, sub-process or risk element is affected depends on its exposure. Both large-scale exposure and local effects may lead to shutdowns, depending on whether sub-processes and risk elements are affected and to what extent.

[20] The Business Continuity Institute 2005, p. 26.

[21] Annex III provides an overview of possible threats and their characteristics as well as further points of contact for analysing these threats. The list of threats in the Annex is limited to natural disasters, technical failure, human error, wilful acts and war. It is not meant to be exhaustive; practitioners should add further types of threats as relevant. In particular, this guide does not cover threats which arise gradually and can lead to financial, market or strategic risks.

- Anticipated intensity:
  How strong will the threat impact be on a sub-process and its risk elements?

- Anticipated duration:
  How long could the incident last?

- Advance warning:
  How much time can be expected between the advance warning and the incident?

- Secondary effects:
  What effects will arise from process dependencies?
  What psychological effects could the incident produce?
  What kind of public or media impact could the incident have?

- Reference incidents:
  Which comparable incidents could be examined for further information?

- Likelihood of occurrence:
  What chance of the incident occurring can be estimated or identified?

Often, the likelihood of a scenario with a pre-determined intensity, geographical scale and duration, advance warning and secondary effects can only be estimated. For example, historical records useful for calculating the probability of an incident have been kept only for certain natural events or failures of man-made structures. When developing scenarios, it is advisable to estimate the probability of occurrence using a classification system.[22]

The selected scenarios should be checked, updated and added to on a regular basis. Further relevant scenarios can be added as needed in order to identify all possible risks to the organization.

### 3.2.2.2 Vulnerability analysis

Along with possible threats, the vulnerability of sub-processes and risk elements is decisive in determining how the organization is affected and what damage occurs. The more vulnerable individual sub-processes and risk elements are, the greater the impact of threats on the organization’s product or services.

A catalogue of criteria is used to identify the vulnerability of sub-processes and individual risk elements. Using the catalogue of criteria, the vulnerability of each risk element in a sub-process is estimated. This can also be done using a classification system.[23]

Organizations can use the following list of criteria to create or add to their own catalogue of criteria.

- Dependence on risk elements:
  If a sub-process depends on a risk element in order to perform its tasks, the potential unavailability or alteration of this risk element makes the sub-process vulnerable. In the risk analysis, this criterion can be viewed as a way to weight the importance of the risk element for the sub-process.[24]

- Dependence on external infrastructures:
  If a risk element depends on an external infrastructure in order to perform its tasks, the potential unavailability or alteration of this infrastructure makes the risk element vulnerable.

**IMPORTANT NOTE – DEPENDENCIES AND SCOPE OF SCENARIO:**
Extreme incidents typically have a broad range of impacts. For example, a power failure may affect the water supply or interfere with suppliers’ operations.

When developing scenarios, one should be careful to view each scenario in isolation, such as scenario 1: Failure of external power supply, scenario 2: Failure of external water supply. Otherwise, the risk analysis will be based on a few very complex scenarios with too many impacts to keep track of.

But marginal effects arising from dependencies should be incorporated into the scenarios. This applies in particular to effects which magnify the impacts.

[22] The example of risk analysis in Annex V uses a five-step classification for the probability of possible scenarios.

[23] The example of risk analysis in Annex V uses a six-step scale of vulnerability (including 0 for not relevant).

[24] In the example of risk analysis in the Annex, this criterion is used as a weighting factor. It is calculated as an individual factor in the risk identification process. Estimates of the remaining vulnerability criteria are added together and therefore treated as a collective factor in the risk identification process.

- Dependence on internal infrastructures:
  If a risk element depends on an internal infrastructure in order to perform its tasks, the potential unavailability of this infrastructure makes the risk element vulnerable.

- Robustness:
  The physical robustness of risk elements (in particular facilities, equipment, buildings) is an important factor for whether they will be damaged by an extreme incident, with effects for the relevant sub-processes.

- Actual level of protection:
  A risk element not sufficiently protected against a threat is vulnerable should this threat arise (example: (non-)existent building security measures).

- Redundancy, substitutes:
  If something should happen to a risk element in an organization, it is easier to handle the situation if there are backups or substitutes to perform the same tasks. Redundancy of risk elements or substitutes reduce the vulnerability of the sub-process in question.

- Restoration effort:
  Restoration effort refers to the effort needed to restore a damaged risk element. With regard to the vulnerability of a sub-process, this covers not only monetary costs, but also the time and staff resources needed.

- Adaptability:
  A sub-process is vulnerable if its risk elements cannot adapt easily or at all to changing framework conditions (example: in the case of hot weather leading the temperature of river water to rise, this could be water-cooled equipment).

- Buffer capacity:
  Buffer capacity means that the sub-process can tolerate the effects of an incident to a certain degree and for a certain time without being affected.

- Transparency:
  Transparency means that it is easy to understand how a risk element is put together and how it functions, so that it can be repaired quickly in case of crisis, for example.

- Dependence on specific environmental conditions:
  Organizations perform under the environmental conditions prevailing at their location. If the organization depends on specific environmental conditions, then it is vulnerable to potential changes in these conditions.

### 3.2.2.3 Risk calculation

Within the risk analysis, calculated values, estimates or results of the scenarios and vulnerability analysis are linked to risk values or results. Risk values are linked by means of a function. In this guide, sub-risks to risk elements are understood as a function of the probability that the scenario in question will occur and of the vulnerability of the risk element. The overall risk to a sub-process is then the aggregate of sub-risks to the risk elements in the sub-process.

In principle, risks can be calculated in three different ways: [25]

- Qualitative risk calculation: This method delivers rough estimates of described risks in text form, without producing numerical comparability.

- Semi-quantitative risk calculation: This method uses a classification system to estimate values for individual risk factors so that they can be compared in numerical form.

- Quantitative risk calculation: This method calculates risk factors mathematically, for example by using time-series analyses in the case of probability of occurrence, or by using simulation models to identify the impacts on an organization.

The choice of method depends on how much effort can and should be expended, and on what information is available.[26]

### 3.2.2.4 Comparing and evaluating risks

The risk values or described risks calculated in this way can now be compared with each other. Such comparison is especially useful in the case of qualitative and semi-quantitative analyses, because the resulting values and descriptions are not absolute quantities. But the results of qualitative and semi-quantitative analyses can be very valuable in relation to each other, i.e. in internal comparison.

The aim of such comparison is to identify those risk elements and sub-processes which face the highest risks.

[25] Cf. Australian/New Zealand Standard 2004, pp. 18–19.

[26] Annex V gives an example describing how to carry out a risk analysis using semi-quantitative calculation of sub-risks to risk elements and of overall risks to sub-processes. For another method of risk analysis specifically for the field of information technology, see: Bundesamt für Sicherheit in der Informationstechnik (BSI) 2005.

The risk evaluation should indicate whether the protection aims initially defined can be achieved given the existing risks. If there are too many high sub-risks, operational protection aims should be formulated to serve as the starting point for taking preventive measures. Examples of operational protection aims are

- reducing the overall risk to sub-process X, and
- reducing the highest sub-risks for all sub-processes which are part of critical processes.

The highest priority should be to take measures for the sub-processes displaying the greatest sub-risks.

It is ultimately the task of the organization’s decision-makers to choose the appropriate operational protection aims and measures.

## 3.3 Phase 3: Preventive measures and strategies

Preventive measures help reduce risks to critical processes. They help achieve operational protection aims and thus raise the threshold for potential crises in the organization (see also Figure 5). This can reduce the number and/or intensity of crisis incidents.

Preventive measures should be subject to a cost-benefit analysis aimed at reducing the overall risk. This is done by comparing potential expenditures and the direct and indirect costs resulting to the organization from an extreme incident. Combining the results of a risk analysis with those of a cost-benefit analysis leads to the selection of measures which are especially efficient within the framework of the existing budget.[27]

However, measures to reduce risks that are unlikely to occur but would have dramatic impacts if they did are often impossible to justify on the basis of risk and cost-benefit analysis alone. In such cases, it may help to consider societal and ethical aspects as well as the legal framework conditions when deciding on protective measures.

Preventive strategies take advantage of the tools of risk avoidance, risk shifting and risk acceptance. They should only be used in tandem with risk-reduction measures, because they may severely limit the organization's flexibility (risk avoidance), or they may not help reduce physical risks (risk shifting, risk acceptance).

### 3.3.1 Risk reduction

Risk-reduction measures reduce either the vulnerability of risk elements to threats or directly address the business continuity of critical processes by creating redundancies or substitutes. Redundant systems or substitutes enable critical processes to continue operating under recovery management even if risk elements have been affected. [28]

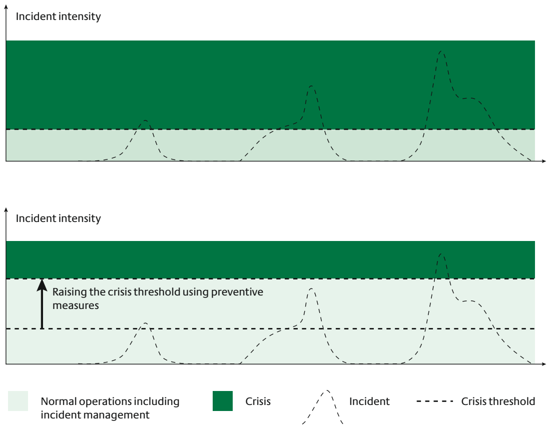
### 3.3.2 Risk avoidance

Risks can be avoided, either by avoiding regions where threats exist or by taking measures to ensure that threats do not arise.

It is often possible to identify areas exposed to natural threats or high-risk facilities (e. g. transport routes for hazardous cargo). Such areas can be avoided when planning new sites or the construction of new buildings or facilities.

However, it is impossible to avoid all risks, as no location is entirely risk-free.

Figure 5: Incident intensity and crisis threshold


Incident intensity
Incident intensity
Raising the crisis threshold using preventive measures
Normal operations including incident management
Crisis
Incident
Crisis threshold

[27] Cf. Australian/New Zealand Standard 2004, pp. 21–22.

[28] Annex IV.1 contains an extensive checklist for implementing preventive measures.

### 3.3.3 Risk shifting

Risk shifting transfers risks to other enterprises or contract partners in order to reduce the financial impact on one's own organization in case of damage. Risk-shifting instruments include the following:

- shifting risk to insurers, and
- shifting risk to suppliers or clients.

**IMPORTANT NOTE:**
Shifting risk does not reduce physical risks to persons or goods. It only affects the financial consequences to the organization of any damage sustained.

### 3.3.4 Acceptance of risks (residual risks)

Preventive measures and strategies pursued by the organization raise the overall security level. Yet certain risks cannot be overcome entirely. The remaining residual risks should be documented and the organization's willingness to accept them should be recorded in writing.

Residual risks can lead to crises which typically overwhelm normal operations. A system of crisis management is needed to enable the organization to deal with such situations effectively.

### 3.3.5 Property insurers' experience with damages

Property insurers naturally have a special interest in protecting against property damage and in reducing the impact of damage incidents on business continuity.

Conclusions drawn from various damage incidents are collected in numerous publications (manuals, guidelines and fact sheets) of the German Insurance Association (GDV).[29] These can serve as additional information sources to optimize the protection of individual organizations and facilities, thereby helping to protect critical infrastructures.

## 3.4 Phase 4: Crisis management

In this guide, a crisis is defined as a deviation from the normal situation which cannot be handled using normal operating procedures. Crises in critical infrastructure organizations can have serious consequences for the functioning of enterprises and government authorities and thus result in harm to the public or to disruption of the political, social or economic system. The Trading (Control and Transparency) Act (KonTraG) uses the term "threat to existence", which is very useful for defining crises.[30] A crisis should be clearly distinguished from less serious incidents, referred to in this guide as disruptions (see Figure 5, page 21).

Crises may originate within the organization itself, for example financial crises as the result of mismanagement or fraud (see Figure 6). External triggers for crises include stock market crashes, negative media coverage or supply difficulties. Other major triggers for crises in critical infrastructures include natural disasters, technical failure, human error, wilful acts of a terrorist or criminal nature, and armed conflicts.

Crisis management plays a major role in protecting organizations and thus critical infrastructures and the public. Crisis management cannot be separated from risk management. Conceptual, organizational, procedural and physical preparation for crises is based in part on the results of risk management. The nature and extent of residual risks identified by risk management can, in some cases, influence the type of preparation carried out as part of crisis management. Because risk-reduction measures cannot reduce all risks and some residual risk always remains, crisis management deals with crises that prevention alone cannot avert.

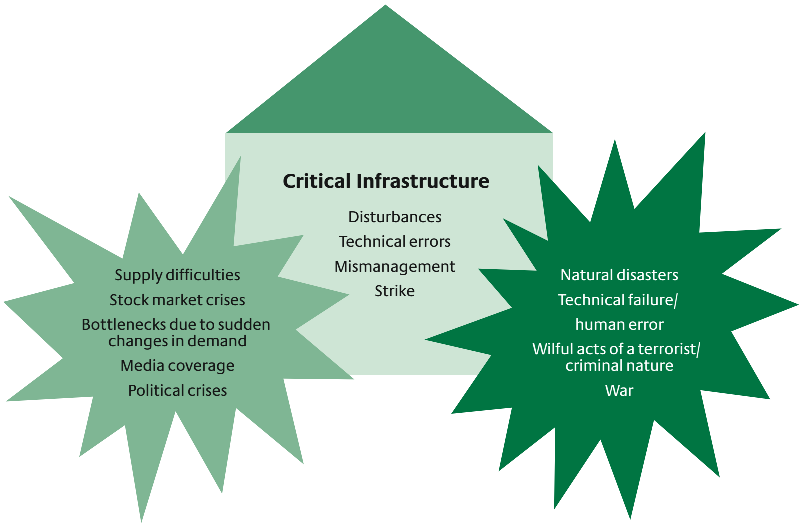
The aim of crisis management for critical infrastructure organizations is to deal with a crisis while

- maintaining the greatest possible ability to function, and/or
- recovering critical functions as quickly as possible.

[29] Cf. VdS-Richtlinien 2007, for example.

[30] Cf. Trauboth 2002, p. 14 f.

**Figure 6: Internal and external crisis triggers**

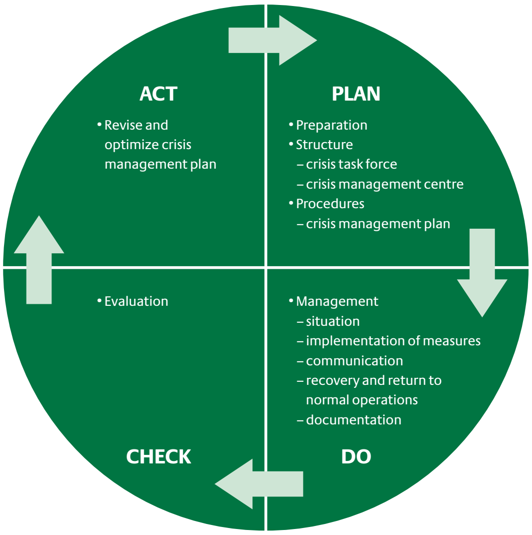


Successful crisis management is embedded within other management strategies, such as risk management described above. Crisis management involves preparing and activating measures to keep the organization functioning and to ensure business continuity and a return to normal operations. Evaluating the crisis management system during and after an incident makes it possible to improve and refine the system. Crisis management can thus be understood as a PDCA cycle within risk management. The crisis management process is shown in Figure 7.

The most important tasks of crisis management are:

- creating the conceptual, organizational and procedural conditions needed to deal with an extreme incident as effectively as possible, and
- establishing special structures to respond in case of crisis, in particular setting up a crisis task force.

**Figure 7: The crisis management process**[31]



[31] Annex IV.2 contains detailed checklists to help prepare for crises.

The most important features of crisis management are the following:

- Crisis management is a process which includes planning, implementation and evaluating a plan and the resulting action in order to respond effectively and efficiently to a crisis.
- As a rule, measures are taken using the limited resources and information available.
- External support or resources may be needed.
- Decisions have to be made quickly and on the basis of incomplete information.

### 3.4.1 The structure of crisis management

The basic elements of crisis management are a special structure to take action in case of crisis and scenario-based plans to ensure business continuity. All preliminary planning necessary and possible for this purpose is compiled in a crisis management plan.

#### 3.4.1.1 The crisis management plan

The crisis management plan lists all crisis-relevant structures and planned measures to be carried out by organization staff responsible for crisis management and business continuity. A good crisis management plan is short and precise. Crisis checklists[32] make it easier to ensure that all the necessary measures are carried out and no important tasks are forgotten.

A crisis management plan covers the following points and indicates who is responsible for them[33]:

- Purpose, aim and scope of the crisis management plan
- Legal foundations
- Development of a special crisis organization
  - crisis task force
  - definition of tasks, areas of responsibility and competences, including the job titles responsible[34]
  - specific crisis management responsibilities and activities
- Development of special procedures to deal with crises, return to normal operations and post-crisis follow-up
  - chain of command and alert
  - models of escalation and de-escalation
  - contact information for contacts within and outside the organization
  - incident-specific measures for recovery and return to normal operations
  - information on post-crisis follow-up
- Development of scenario-based plan components, for example
  - evacuation
  - power failure
  - pandemic
  - IT and/or CT failure

The crisis management plan must be updated and practice drills conducted regularly.

**IMPORTANT NOTE:**
A crisis management plan should always be drawn up, even if many preventive measures have already been implemented.

[32] Annex IV.2 contains detailed checklists to help prepare for crises.

[33] For an example of a crisis management plan or emergency handbook in the IT field, see: Bundesamt für Sicherheit in der Informationstechnik (BSI) 2008.

[34] Jungbluth 2005, p. 15.

### 3.4.1.2 Special crisis structures

Crisis situations require special structures. A crisis task force has the goal of dealing with crises as quickly and competently as possible. The structure of the crisis task force depends on the type and needs of the critical infrastructure organization.

#### 3.4.1.2.1 Crisis task force

The crisis task force is the central instrument of crisis response. It is a special structure that overrides the normal operating procedures in order to deal with special situations in the affected units; in it, competences from different departments are brought together under a single leadership. A crisis task force is a decision-making tool which also performs coordinating, informing, advising and support functions. The crisis task force is made up of a leader[35] and the task force team. Within the crisis task force team, one may distinguish between

- the core team, made up of the leader and up to three team members with key functions,
- the extended team, made up of persons with designated special functions or supporting groups,[36] and
- specialists to advise the task force.

All appointed and trained task force members and their deputies must be familiar with their specific tasks and ready to carry them out. When choosing deputies, it is also important to remember those scenarios in which high rates of absenteeism may affect the task force (e. g. major epidemics or pandemics).[37] In order to deal with such situations, several deputies should be designated.

Before a crisis occurs, special work-time arrangements (shift system) should be made specifically for the task force in case of crisis; these should also include some overlapping time in which the earlier shift can update the shift coming on duty of the latest developments. Crises are periods of high stress, so shifts should not exceed six to seven hours.

A model for crisis task forces has been established in the field of threat prevention and disaster preparedness; this model is described in detail in the Fire Brigade Regulation 100.[38]

This model originated in a military context; it describes the form and functions of a command staff and is directed at all organizations whose activities are primarily operational-tactical.

In the field of disaster preparedness on public administration level, a management task force acts alongside the operational-tactical command staff to handle administrative and organizational tasks. The management task force supports the operational-tactical components and carries out primarily administrative tasks. In case of crisis, the management task force may also act on its own if no operational components are deployed.

The form and functions of a task force in private enterprises and government authorities outside the field of threat prevention and disaster preparedness depend on the organization's needs in the event of a crisis. In some enterprises, it may make sense to organize the task force along the lines of a command staff or management task force, for example if the enterprise performs similar tasks or when close collaboration with disaster preparedness staff is needed. Other enterprises and government authorities may choose other ways to structure their task forces.[39] The important thing is to ensure that the critical infrastructure operator is able to communicate with the threat prevention authority/disaster preparedness organizations. Here, an intensive staff exchange between task forces is helpful and should be an explicit requirement for management task forces.

The following functions/tasks should be covered by every task force, no matter what the organization's tasks are[40]:

- managing all personnel-related aspects,
- gathering and regularly updating information on the situation,
- delegating tasks to resolve the crisis and coordinating the necessary operations carried out by organization staff,
- handling media and public relations,
- managing all aspects of information and communications, and
- providing for the needs of crisis management staff.

[35] The crisis task force may be headed by the same person who heads the enterprise or government agency. However, this is not advisable, as having different people for these tasks gives the decision-making level more leeway to make important and independent decisions.

[36] Cf. Trauboth 2002, p. 45.

[37] Measures to protect staff, in particular the crisis task force include ensuring adequate hygiene, providing protective masks and setting up the capacity to work from home. For more information, see Bundesamt für Bevölkerungsschutz und Katastrophenhilfe 2007, Robert Koch Institut 2005 and 2007a and Annex IV.2.

[38] Feuerwehr-Dienstvorschrift 1999.

[39] One possible alternative for IT-related organizations is described in BSI-Standard 100-4. See Federal Office for Security in Information Technology (BSI) 2008.

[40] Revised in line with Feuerwehr-Dienstvorschrift 1999.

In private enterprises, crisis task forces may also cover the following functions:

- legal affairs,
- finance/budget,
- marketing,
- logistics,
- quality management,
- sales and distribution,
- site security,
- environmental protection,
- security of facilities,
- toxicology,
- the company's fire brigade and
- emergency medical service.

Task profiles for each function can be prepared ahead of time, describing the general duties arising in every crisis management situation.

In the case of enterprises or companies with international operations and government authorities with direct international relations, it may make sense to include the function "international relations". It may also be worth considering assistance for the task force, especially in drawing up situation reports.

If the enterprise or government authority has several locations, branches or field offices, then in addition to on-site task forces it may be useful to have an overall task force to deal with crises affecting the entire organization.

#### 3.4.1.2.2 Crisis task force leadership

In the event of a crisis, the head of the crisis task force oversees all crisis response-related activity. He/she is responsible for making all crisis-management decisions and should therefore already hold a leadership position in the enterprise or government authority. The head of the crisis task force needs a predetermined legal and financial framework in order to perform his/her tasks.

Leading a crisis task force requires a strong character and extensive experience. This position requires strong leadership and interpersonal skills as well as the ability to perform well in extreme situations, to make decisions under pressure and to work as part of a team. The task force head must also be able to grasp and analyse information quickly. He/she must also have the confidence of the organization's leadership and the entire crisis task force team. It is helpful for task force heads to be generalists who are in charge of specialists.

It is advisable for task force heads to take part in basic and advanced training to gain specific crisis management skills.

#### 3.4.1.2.3 Crisis task force team

Depending on the type of crisis, incident-specific special functions will be added to the existing core team. These special functions will be performed by persons with specific skills. The need depends on the type of crisis. The head of the task force is responsible for selecting the task force team. The core team's task is to prepare decisions for the task force head and to organize measures to deal with the incident or limit damage.

#### 3.4.1.2.4 Expert advisers in the task force

Internal and external experts can be added to the task force as adjunct members. They can be included in particular in decision-making processes where expert information is needed, such as information about operating procedures, software used, security procedures, finances, environment, production, fire and emergency services and disaster preparedness at local, state and federal level.

### 3.4.1.3 Procedures

The activation of crisis management and the duties of the task force are governed by certain procedures. This is reflected in the special task force functions that are performed by the appropriate appointed staff.

The following tasks are performed as part of crisis management:

- informing, reporting and alerting;
- assessing the situation and forecasting likely developments, including gathering information;
- developing specific strategies for managing the crisis and seeing that they are implemented;
- overseeing and monitoring the implementation;
- documenting the action taken;
- communicating, internally and externally, what action has been taken;
- activating measures to restore operations;
- restoring business continuity.

#### 3.4.1.3.1 Reporting channels and alerts

In a crisis, successful crisis management depends on the rapid and sufficient flow of information. Most of this flow consists of reports, both oral and written. High-quality reporting makes it easier to manage crises. Reports should[41]

- be made without delay,
- include when and where the information came from,
- be clear and to the point,
- be concise but contain all essential information,
- clearly distinguish between facts and suppositions, and
- be prioritized according to urgency.

[41] Feuerwehr-Dienstvorschrift 1999, p. 29.

A standard channel for internal reporting of incidents and damage should be established along with standard reporting procedures ensuring that all necessary information is gathered and forwarded.

If an incident occurs which the in-house incident management is unable to handle alone and which may develop into a crisis, then the head of the task force must be informed as quickly as possible. Organization staff, clients, the public or other enterprises and government authorities may provide information about damage affecting the organization. Depending on the scale of the incident, someone with decision-making authority, typically a supervisor, should be informed. If the incident cannot be managed within the supervisor's area of responsibility, he/she reports it to the head of the crisis task force or the head of the organization. The head of the crisis task force decides whether to activate the task force and special procedures.

The head of the crisis task force assesses the danger and alerts the persons active in crisis management or units such as the core team, the extended crisis task force, the control centre and the head of the enterprise or government authority. Others outside the organization are informed of the incident as needed, e. g. suppliers and clients, organizations and aid agencies, public institutions such as schools and kindergartens, government authorities and offices and the public health service (also physicians and hospitals, if necessary).

Alerts are sent out on the basis of call lists containing contact information for the staff involved in crisis management and relevant contacts outside the organization. The lists of persons to alert or inform should be compiled by the organization ahead of time and kept up to date.

Switching from normal operations to crisis management mode and alerting staff can take place all at once or in a process of escalation. Here, the following two models are conceivable:

- Threshold model
  In this case, there is only one alert level separating normal operations (including incident management) from crisis management. Crossing this threshold automatically leads to a situation in which the crisis management plan is activated and the crisis task force assumes control of the crisis. All staff and relevant units involved in crisis management are alerted.

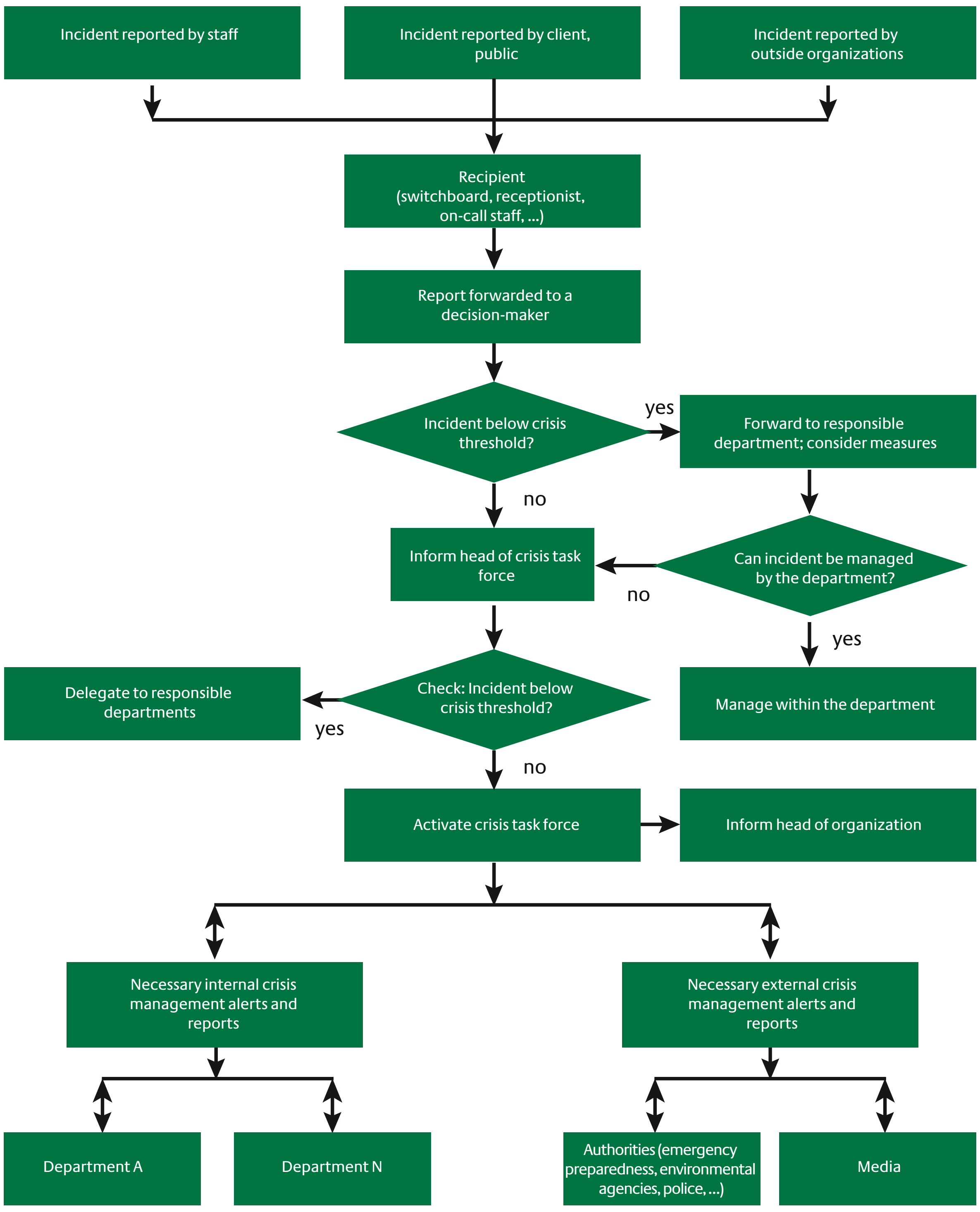
- Escalation model
  In this case, the crisis management plan is divided into several stages of alert. The deployment of staff and material resources and the measures taken depend on the incident. This model allows a targeted response to possible incidents and their impacts but it requires more complex crisis planning.[42]

After an incident has been reported to the head of the crisis task force and the relevant units within and outside the organization have been alerted, the crisis task force assigns tasks within the organization. The staff involved in crisis management report to the task force on the situation. As a rule, external agencies communicate directly with the crisis task force.

Figure 8 “Reporting channels and alerts” (page 28) gives an overview of reporting channels within an organization and the alerting of relevant persons.

[42] Jungbluth 2005, p. 17.

**Figure 8: Reporting channels and alerts**


Incident reported by staff
Incident reported by client, public
Incident reported by outside organizations
Recipient (switchboard, receptionist, on-call staff, ...)
Report forwarded to a decision-maker
Incident below crisis threshold?
yes
Forward to responsible department; consider measures
no
Inform head of crisis task force
no
Can incident be managed by the department?
yes
Delegate to responsible departments
yes
Check: Incident below crisis threshold?
Manage within the department
no
Activate crisis task force
Inform head of organization
Necessary internal crisis management alerts and reports
Necessary external crisis management alerts and reports
Department A
Department N
Authorities (emergency preparedness, environmental agencies, police, ...)
Media

**3.4.1.3.2 Crisis communications**

Crisis communications include informing the public, particularly the media, about the crisis. This is the task of the press and public relations department.

In the critical early stage when a crisis is developing, it is crucial to keep other organizations, the media and the public as well as one's own organization informed. The work of informing the public about the crisis must start at the same time as the crisis management effort. Information for the press must be released within the shortest possible time. However, keeping certain information confidential is also part of crisis communications, so it is especially important to identify information that needs to be kept confidential.

For crises that affect the public, hotlines and user-friendly websites should be prepared. Specially trained staff, including backup staff, must be immediately available in case of crisis in order to manage the increased demand for public information. During this phase, it is also essential to intensify internal communications.

The media are often the first to report on an incident or crisis. For this reason, at least one press spokesperson should be designated in advance to handle all relations with the media. Contact with reporters therefore arises already in the earliest phase of the developing situation. Perceptions of the crisis and the image of the crisis management operation depend greatly on the media reporting. Effective and efficient media relations therefore require the following:

- an established network with local, regional and national media,
- recommendations for initial media contacts at the start of a crisis,
- background information and sample press releases, talking points, etc.,
- experience with press conferences and special media training, as well as
- outside support from crisis communications specialists as appropriate.

During a crisis that affects the public, it is important for responsible decision-makers (chief executive, head of the government authority, organization spokesperson or head of public information) not to wait too long before speaking to the media as appropriate to the situation. Public statements must be formulated in a balanced way and present information accurately, clearly and understandably.

The basic rules for external crisis communications:

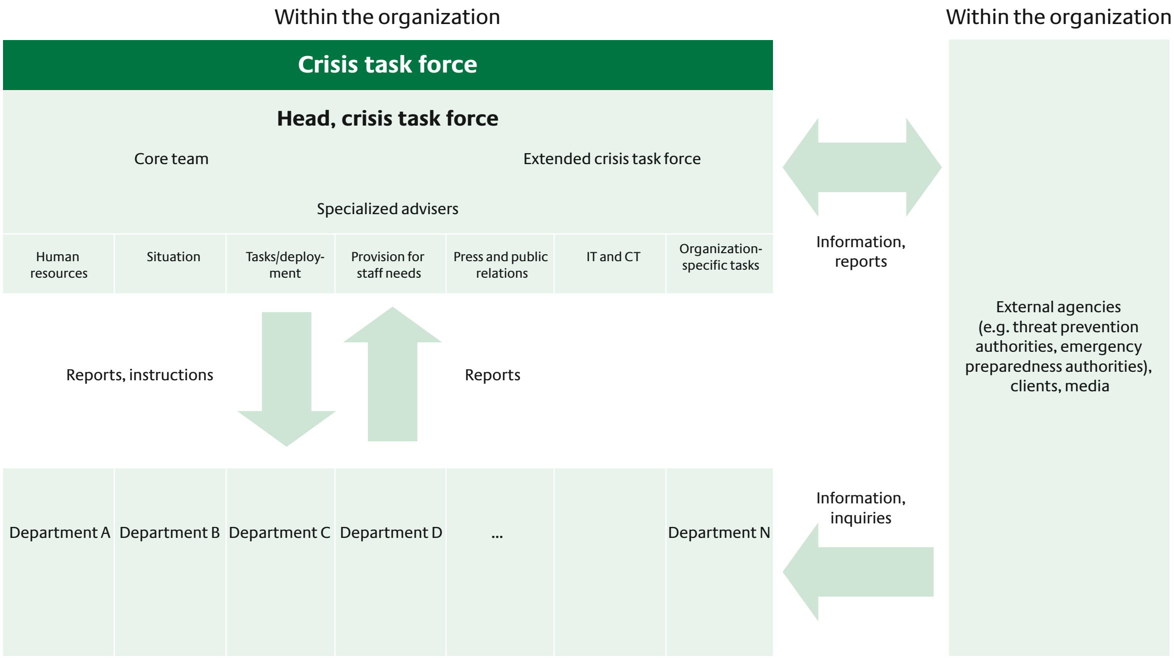
- Every crisis is also an information crisis.
- Crisis management is also information management.
- The first hours in a crisis are decisive: Information conveyed during this phase will make a more or less lasting impression.
- The quality of crisis communications will largely shape the public's view as to whether those responsible are capable of managing the crisis or not.
- The information provided must satisfy public needs.
- Those responsible for providing information should make the crisis task force aware of the information needed by the public and the media and of the impact of such information.

**IMPORTANT NOTE:**
It is important to make sure that information to the public is provided by authorized personnel only.

In case of long and difficult incidents, it is advisable for a member of the organization's leadership to handle external communications. The crisis task force then provides this person with the latest information and with intensive advising. In this case, the head of the crisis task force assumes responsibility for coordinating internal crisis management and continues to make all decisions.

The following chart (figure 9, page 30) summarizes the structure of the crisis task force and special crisis procedures.

Figure 9: Crisis task force and special procedures



### 3.4.1.4 Crisis management centre

The crisis management centre is the room specially reserved for the crisis task force before, during and after a crisis. It may also be called a situation room or crisis management conference area.

The crisis management centre is where members of the crisis task force come together. When planning and furnishing this room, the following aspects should be considered: location, backup location and equipment/furnishings.

The location should be decided on ahead of time; it should be easily accessible and be protected against possible threats. In case there is a loss of function at the primary location, an alternative location should be available; if appropriate, only the organization's leadership, the crisis task force and its head should be informed of its existence and location.

The crisis management centre should be equipped with a redundant communications and information infrastructure as well as effective technology for gathering, processing and presenting information. Backup power for all technical equipment and lighting should be available.[43]

And security should also be guaranteed, for example protection against surveillance and electronic eavesdropping. The functionality of the room and its equipment should be checked regularly.

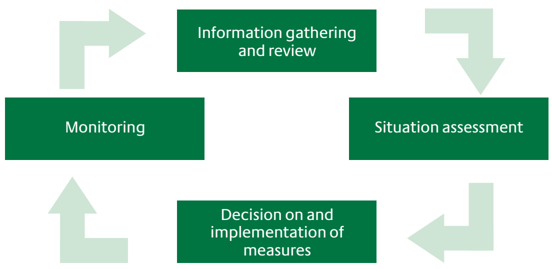
The type and extent of the crisis task force's personnel, space and technical resources and the room for the crisis situation depend on the existing threats, the type and scope of tasks and processes, the size and diversity of the organization, on local circumstances and on whether it is the organization's headquarters or branch location.

### 3.4.2 Crisis management

After the crisis task force is activated, crisis management tasks begin. The task force meets in the crisis management centre and takes action based on the crisis management plan. Information and communications connections are crucial to crisis management; they must be functioning (or have been restored). All actions and decisions taken as part of crisis management operations should be documented from the time the crisis task force begins its work.

[43] Please see Annex IV.6 for a detailed list of space and technical requirements and other equipment/furnishings for the crisis management centre.

Figure 10: Cycle for managing extreme incidents[44]


Information gathering and review
Situation assessment
Decision on and implementation of measures
Monitoring

Managing an extreme incident follows a circular pattern consisting of the following steps: gathering information on the situation, assessing the situation, deciding on and taking action and monitoring the effects of this action. This cycle is carried out following each new sub-incident and each measure that significantly changes the crisis situation until the normal situation resumes.

### 3.4.2.1 Information gathering and review

**Collecting information**

The crisis task force gathers information on the incident. A situation report is compiled based on the information gathered. This report is needed in order to make a reasonable assessment of the crisis and to decide on what action to take to minimize damage. The situation report describes

- the type, extent and sequence of events,
- the effects and possible development of the situation,
- options for response, and
- action taken so far.[45]

The report draws on all previous reports and personal investigations. Information about the threat and damage situation and the organization's own staffing and technical capacities are also needed.

Gathering maps ahead of time helps with information collection during the crisis management phase. The information collected should include the following:

- maps and site diagrams (buildings and grounds),
- building floor plans (fire extinguishers, exits, emergency exits, escape routes, shelter, crisis management centre), and
- plans and diagrams of facilities and utility systems (main switch for electricity supply, main shut-off valves for water and gas, location of pipes).

These maps and diagrams should be updated regularly.

**Means for collecting and processing information**

The information collection is based on reports from organization staff, clients and the public, external private and public actors (e. g. clients, police, emergency response staff), and from the media.

Some of the resources necessary for collecting information are the same as those needed in the crisis management centre:[46] for example telephones, Internet, radio and television sets, as well as reference books and the maps and diagrams mentioned above.

Presenting the information in graphic form helps all those involved grasp it intuitively. If the organization uses a geographic information system (GIS),[47] key spatial information can be filed ahead of time and presented electronically.

**Presenting the situation report**

The crisis task force draws up a current situation report based on the following factors as appropriate: place, time, weather, damage incident/threat situation, measures initiated and further options for response.[48] It compiles all previous reports and information received into a concise overview of the current status. Important components of the situation report include:

- area maps,
- building plans,
- incident reports and
- video and audio recordings.[49]

The most important points of information gathering and review are summarized in the following figure (see page 32).

[44] Taken from Feuerwehr-Dienstvorschrift 1999, p. 25.

[45] Jungbluth 2005, p. 38.

[46] See Annex IV.6.

[47] Geographic information systems are database-supported software products that can be used to collect and analyse spatial data

[48] Feuerwehr-Dienstvorschrift 1999, p. 26.

[49] Adapted from Feuerwehr-Dienstvorschrift 1999, p. 41.

**Figure 11: Overview of information for the situation report**[50]

**Incident**
- type of damage
- cause of damage

**Object of damage**
- type
- size
- material
- construction
- surroundings

**Extent of damage**
- humans
- functionality
- animals, environment
- material assets
- production processes
- organization's ability to function
- indirect damage

**Crisis management**
- head of crisis task force
- crisis task force

**Staff with responsibilities in case of crisis**
- strength
- availability
- additional training (e.g. first aid)
- productivity

**Means**
- IT
- vehicles
- equipment

### 3.4.2.2 Situation assessment, decision-making and implementation of measures

The situation report is systematically assessed, leading to a decision on further measures. After assessing the situation, the head of the crisis task force decides on the next steps.

The following are used in making the situation assessment[51]:

- the situation report,
- the legal basis,
- guidelines and
- fact sheets.

The situation should be discussed regularly, if necessary in situation briefings. The head of the crisis task force must make definite decisions to implement measures in all conceivable crises.[52]

### 3.4.2.3 Monitoring

Monitoring is used to determine whether the instructions given by the crisis task force have in fact reached the relevant staff (e. g. branch office or emergency staff) and whether they have understood and acted on them correctly. Monitoring is also used to keep track of the effects of decisions.

After a measure is taken, a new situation results, which is then described and presented in the situation report. The new situation report serves as the basis for monitoring the effects of the measures taken at this point and for planning the next steps.

### 3.4.2.4 Ensuring continuity of operations

A key element of crisis management in critical infrastructure organizations is activating emergency measures, redundant systems and substitute systems identified and installed during the risk management process as preventive measures to ensure continuity of operations.[53]

### 3.4.2.5 Return to normal operations

The head of the crisis task force is responsible for activating and deactivating the crisis management system and for returning to normal operations. Here too, a threshold model or de-escalation model is conceivable.[54] In a threshold model, the transition to normal operations takes place without delay; in a de-escalation model, the transition occurs in stages. The latter model is likely to be applied in most crisis situations, especially those with impacts on various areas of the organization.

### 3.4.2.6 Documentation of crisis management operations

All incoming and outgoing reports (e. g. via telephone, fax, e-mail) and all decisions, measures and activities should be documented in writing. Here, standard forms indicating the date and name of the processing staff member may be helpful. Other aids to documentation include:

- pre-printed forms,
- proof of sending and receipt,
- incident logs,
- report logs and
- electronic media.

Documentation during a crisis aids in evaluation and in clarifying financial, insurance and legal matters. Documentation should therefore be able to withstand judicial scrutiny.

[50] Taken from Feuerwehr-Dienstvorschrift 1999, p. 27.

[51] Taken from Feuerwehr-Dienstvorschrift 1999, p. 45.

[52] Annex IV.3 contains checklists of initial measures for selected crisis situations.

[53] See Chapter 3.3.1.

[54] See Chapter 3.4.1.3.1.

### 3.4.3 Follow-up

After the return to normal operations, the documentation is used to follow up on the crisis management operation. Such follow-up may take the form of a report drafted by the head of the crisis task force soon after and in confidential form and provided to the head of the organization. This report serves the organization leadership as a basis for evaluating any legal consequences for the organization or staff deployed. Another important objective of follow-up is checking the functionality and practicality of the crisis management plan for gaps in order to remedy them.[55]

### 3.4.4 Exercises

As a rule, extreme incidents occur very rarely. Crisis structures and procedures should therefore be practiced at regular intervals to ensure that they function smoothly during a crisis. The aim of such exercises is:[56]

- to check whether the crisis management plan is effective and workable,
- to practice crisis coordination and communication, and
- to test crisis-specific procedures.

There are various kinds of exercises involving different levels of abstraction and different amounts of effort, including:

- **table top exercises** (participants: members of the crisis task force; managing a damage scenario in theory);
- **extended table top exercises** (participants: members of the crisis task force and other areas; managing a damage scenario in theory);
- **full-scale exercises** (participants: all executive levels and offices; actually working through an exercise scenario);
- **functional drills** (e. g. evacuation drills, communication training);
- **alert drills** (to determine availability and time needed for operation readiness).

Criteria for choosing a particular type of exercise are:

- the stated objective,
- the desired interval at which the exercise is to be held, and
- the amount of effort planned.

Full-scale exercises which include all management levels and staff are the most realistic; however, they also require a great deal of effort for planning and execution.

By contrast, table top exercises and extended table top exercises cover the theoretical management of damage scenarios. Table top exercises practice the core areas of crisis management, such as the crisis task force and the functionality of the crisis management plan. Extended staff exercises include other areas such as additional decision-making and reporting channels.

In table top exercises and extended table top exercises, all aspects of an incident are practised with the help of a script, which those in charge of the exercise use to monitor and steer the exercises. As a rule, those participating in the exercise are not familiar with the script, which anticipates possible reactions by participants. Those in charge can incorporate unanticipated reactions into the exercise at short notice.

The disadvantage of table top and extended table top exercises lies in their theoretical nature. Nonetheless, such exercises make it possible to practise strategic core areas of crisis management without requiring the efforts of a full-scale exercise involving the entire staff.

Functional drills may pursue selected objectives, requiring less planning effort than full-scale exercises.

Alert drills test alert system planning and the threshold or escalation model.

Preparation for each type of exercise should answer the following questions:[57]

- What kind of exercise has been chosen?
- What are the objectives of the exercise?
- Who should participate in the exercise?
- Who should be responsible for steering the exercise?
- When and where should the exercise take place?
- What technical aids are needed to carry out the exercise?
- What aspects should the exercise script cover?
- How will the exercise be documented and evaluated?

At the end of the exercise, documentation will check the participants' reactions and whether the crisis management plan was implemented without difficulties. In this way, weaknesses can be identified and the crisis management plan can be revised.[58]

[55] Annex IV.4 contains a list of initial concrete steps for follow-up and analyses the options for preparing for a possible new crisis. For more information, see for example Bundesamt für Sicherheit in der Informationstechnik (BSI) 2006.

[56] Gustin 2004, p. 226.

[57] Gustin 2004, p. 262.

[58] Annex IV.5 contains a checklist on crisis exercises.

## 3.5 Phase 5: Evaluating risk and crisis management

Evaluation covers all phases of risk and crisis management, from checking the items identified during preliminary planning, to checking whether risk profiles are current and whether preventive measures taken and the crisis management system are effective. Such an evaluation should be carried out regularly, preferable once a year.

Additional evaluations are necessary

- after measures have been implemented,
- after expansion or restructuring of the organization, and
- if the threat situation changes.

Risk and crisis management must be taken seriously. Risk and crisis management can provide long-term added value only if all phases are regularly tested, thereby laying the groundwork for continuous optimization of the organization's level of security.

# Annex

# I. References

**American Water Works Association (2001) (ed.):** Emergency Planning for Water Utilities, Manual of Water Supply Practices M19. Denver.

**Australian/New Zealand Standard (2004) (ed.):** Risk Management AS/NZS 4360:2004. Standards Australia/Standards New Zealand. Sydney/Wellington.

**Bockslaff, K. (1999):** Die eventuelle Verpflichtung zur Errichtung eines sicherungstechnischen Risikomanagements. In: NVersZ. No. 3, p. 104–110.

**Bockslaff, K. (2004):** Sicherheit – ein Beitrag zur Wertschöpfung im Unternehmen. In: WIK – Zeitschrift für die Sicherheit der Wirtschaft. No. 5, p. 27–32.

**British Standard (2006) (ed.):** DPC BS 25999-1 Code of practice for business continuity management. London (draft).

**Department of Health and Human Services and the Centers for Disease Control and Prevention (2007):** Business Pandemic Influenza Planning Checklist. http://www.pandemicflu.gov/plan/workplaceplanning/businesschecklist.html (15 October 2007).

**Department of Homeland Security (2006):** Pandemic Influenza Preparedness, Response, and Recovery Guide for Critical Infrastructures. http://www.pandemicflu.gov/plan/pdf/cikrpandemicinfluenzaguide.pdf (15 October 2007).

**Dost, S. (2006):** Risk Management – Features of corporate risks and the likelihood of identification. Innovation and Technical Progress: Benefit without Risk? In: Book of Abstracts of the 15th Annual Conference of the Society for Risk Analysis (Ljubljana, 11-13 September 2006), p. 21.

**Egli, T. (1999):** Richtlinie Objektschutz gegen Naturgefahren. St. Gallen.

**Federal Emergency Management Agency (2003) (ed.):** Risk Management Series Reference Manual to Mitigate Potential Terrorist Attacks Against Buildings – FEMA 426. http://www.fema.gov/plan/prevent/rms/rmsp426 (15 October 2007).

**Federal Environmental Agency, UBA (2001a):** Checklisten für die Untersuchung und Beurteilung des Zustandes von Anlagen mit wassergefährdenden Stoffen und Zubereitungen; Nr. 10 Betriebliche Alarm- und Gefahrenabwehrplanung. http://www.umweltbundesamt.de/anlagen/jeg/downloads/deutsch/check10_bagap_rev00.pdf (15 October 2007).

**Federal Environmental Agency, UBA (2001b):** Checklisten für die Untersuchung und Beurteilung des Zustandes von Anlagen mit wassergefährdenden Stoffen und Zubereitungen; Nr. 11 Hochwassergefährdete Anlagen. http://www.umweltbundesamt.de/anlagen/jeg/downloads/deutsch/check11_hochwasser_rev00.pdf (15 October 2007).

**Federal Ministry of the Interior, BMI (2005):** Schutz Kritischer Infrastrukturen – Basisschutzkonzept, Empfehlungen für Unternehmen. http://www.bbk.bund.de/cln_007/nn_398726/DE/05_Publikationen/05_Fachpublikationen/03_Leitfaeden/Leitfaeden_node.html_nnn=true (15 October 2007).

**Federal Office for Information Security, BSI (2005):** BSI-Standard 100-3 “Risikoanalyse auf der Basis von IT-Grundschutz”. http://www.bsi.bund.de/literat/bsi_standard/standard_1003.pdf (4 October 2007).

**Federal Office for Information Security, BSI (2006):** COMCHECK und ALEX. Beschreibungen, Checkliste und Hilfen für Kommunikationsüberprüfungen und Alarmierungsübungen. http://www.bsi.bund.de/fachthem/kritis/comcheck.pdf (16 October 2007).

**Federal Office for Information Security, BSI (2007):** G 1 Gefährdungskatalog Höhere Gewalt. http://www.bsi.bund.de/gshb/deutsch/g/g01.htm (10 October 2007).

**Federal Office for Information Security, BSI (2008):** BSI-Standard 100-4 “Notfallmanagement”. (to be published online in January 2008).

**Federal Office of Civil Protection and Disaster Assistance, BBK (2005):** Leitfaden für die Errichtung und den Betrieb einer Notstromversorgung in Behörden und anderen wichtigen öffentlichen Einrichtungen. http://www.bbk.bund.de/cln_007/nn_398726/DE/05_Publikationen/05_Fachpublikationen/03_Leitfaeden/Leitfaeden_node.html_nnn=true (15 October 2007).

**Federal Office of Civil Protection and Disaster Assistance, BBK (2007):** Betriebliche Pandemieplanung - Kurzinformation der Bund-Länder-Arbeitsgruppe "Influenzapandemieplanung in Unternehmen". http://www.bbk.bund.de/cln_007/nn_398734/SharedDocs/Publikationen/Publikation_20KatMed/Betr-Pandemieplan,templateId=raw,property=publicationFile.pdf/Betr-Pandemieplan.pdf (15 October 2007).

**Feuerwehr-Dienstvorschrift 100 (1999):** Führung und Leitung im Einsatz – Führungssystem. http://www.idf.nrw.de/download/normen/fwdv100.pdf (15 October 2007).

**Gesellschaft für Anlagen- und Reaktorsicherheit (2007) (ed.):** Managementsysteme in Kernkraftwerken, GRS – 229. Cologne.

**Gray, P.C.R. et al. (2000):** Risk communication in print and on the web. A critical guide to manuals and internet resources on risk communication and issues management. http://www.fz-juelich.de/inb/inb-mut/rc/inhalt.html (4 October 2007).

**Gustin J.F (2004):** Disaster & Recovery Planning: A Guide for Facility Managers. Lilburn.

**International Risk Governance Council (2006) (ed.):** White paper on managing and reducing social vulnerabilities from coupled critical infrastructures. http://www.irgc.org/irgc/IMG/pdf/IRGC%20WP%20No%203%20Critical%20Infrastructures.pdf (15 October 2007).

**Jungbluth, F. (2005) (ed. Euroforum Verlag):** Recht & Haftung für technische Manager, Grundlagen, Aufbau und Methoden eines effektiven Notfallmanagements. Düsseldorf.

**Jungermann, H. et al. (1991):** Risikokontroversen – Konzepte, Konflikte, Kommunikation. Berlin.

**Lewis, T.G. (2006):** Critical Infrastructure Protection in Homeland Security – Defending a Networked Nation. Hoboken.

**National Fire Protection Association – NFPA 1600 (2004) (ed.):** Standard on Disaster/Emergency Management and Business Continuity. Quincy.

**Rahmstorf S. and others (2006):** Der Klimawandel. Munich.

**Robert Koch Institut (2005):** Beispiel von Maßnahmenplanungen im Influenza-Pandemiefall. http://www.rki.de/cln_049/nn_200120/DE/Content/InfAZ/I/Influenza/Pandemieplanung_Konzern-28102005,templateId=raw,property=publicationFile.pdf/Pandemieplanung_Konzern-28102005.pdf (22 October 2007).

**Robert Koch Institut (2007a):** Nationaler Pandemieplan, Teil II. http://www.rki.de/cln_048/nn_200132/DE/Content/InfAZ/I/Influenza/influenzapandemieplan_II,templateId=raw,property=publicationFile.pdf/influenzapandemieplan_II.pdf (6 October 2007).

**Robert Koch Institut (2007b):** Anhang zum Influenzapandemieplan. http://www.rki.de/cln_048/nn_200132/DE/Content/InfAZ/I/Influenza/Influenzapandemieplan_Anhang,templateId=raw,property=publicationFile.pdf/Influenzapandemieplan_Anhang.pdf (6 October 2007).

**Rosenthal, U. (1992):** Crisis management: On the thin line between success and failure. In: Asian Review of Public Administration. Vol. IV No.2, p. 73–78.

**Rössing, R. von (2005):** Betriebliches Kontinuitätsmanagement. Bonn.

**The Business Continuity Institute (2005):** Business Continuity Management, Good Practice Guidelines. www.thebci.org/goodpracticeguidetoBCM.pdf (15 October 2007).

**Trauboth, J.H. (2002):** Krisenmanagement bei Unternehmensbedrohungen. Präventions- und Bewältigungsstrategien. Stuttgart; Munich, Hanover; Berlin; Weimar; Dresden.

**VdS-Richtlinien (2007):** Gesamtprogramm. http://www.vds.de/Gesamtverzeichnis.487.0.html (9 November 2007).

**Verwaltungs- Berufsgenossenschaft VBG (2007) (ed):** Zwischenfall, Notfall, Katastrophe – Leitfaden für die Sicherheits- und Notfallorganisation. Hamburg.

**Wiedemann, P.M. et al. (2000):** Risikokommunikation für Unternehmen. Düsseldorf.

**Zentrum für Alpine Umweltforschung (2000) (ed.):** Leitfaden für erdbebensicheres Bauen. Sion.

# II. Terminology

**IMPORTANT NOTE:**
When drafting this guide, it became clear that risk and crisis management terminology is not yet defined in a standard way. The following list therefore provides definitions of the terms as they are used here, which may differ from their use in other publications.

| Term | Definition |
|---|---|
| **Alert** | Mechanism to inform staff, emergency personnel and the public about an acute threat. |
| **Alert level** | Stage of a situation with regard to measures to be taken. |
| **Business continuity management** | Measures to maintain operations during crisis, e. g. activating a back-up control room.[59] |
| **Civil protection** | Civil measures to protect against, contain and manage the impacts of war, armed conflicts, natural disasters and major accidents. Federal, state and local governments and emergency aid organizations work together to protect the civil population. |
| **Crisis** | An extraordinary situation that occurs despite preventive measures taken by the organization and cannot be managed using standard operating structures and procedures. |
| **Crisis communications** | All acts of communication carried out in connection with a crisis situation to prevent or limit damage, loss of confidence and harm to the organization's image. Crisis communications entails the clear allocation of areas of authority and responsibility and a clear line of communication to ensure uniform content and arguments. |
| **Crisis management** | All activities to prepare for, deal with and follow up on crises. |
| **Crisis management centre** | The room specially reserved for the crisis task force before, during and after a crisis and tocarry out crisis exercises. |
| **Crisis management plan** | Master plan for crisis management covering all measures to be taken in the event of a crisis. |

[59] Von Rössing 2005, p. 426.

| Term | Definition |
|---|---|
| **Crisis task force** | Structure which creates all prerequisites for coordinating all crisis-related activities. |
| **Critical infrastructures** | Organizations and institutions of special importance for the country and its people where failure or functional impairment would lead to severe supply bottlenecks, significant disturbance of public order or other dramatic consequences.[60] |
| **Critical points** | See: areas of vulnerability. |
| **Danger** | Negative impacts on persons, property, and/or the environment caused by threats. |
| **Disaster** | Major incident well beyond the norm which seriously endangers or destroys life, health, property or key infrastructures. |
| **Disturbance** | Departure from the normal situation or process. Causes may be due to internal or external factors. A disturbance can be handled using standard operating structures and procedures. |
| **Epidemic** | High incidence of a disease among a local population. |
| **Escalation model** | Mechanism for assessing the situation and delegating tasks to the crisis management staff.[61] |
| **Evaluation** | Assessment of activities. |
| **Exposure** | The condition of being subject to risk. |
| **Extended table-top exercise** | Table top exercise involving additional levels of the organization (e. g. the relevant departments). |
| **Extreme incident** | A rare event that departs significantly from the norm and may lead to crises. |
| **Incident management** | Conceptual, organization, procedural and physical conditions of the standard operating structures and procedures enabling the optimal handling of disruptions. |
| **Individual vulnerability** | Refers in this guide to one risk element and one vulnerability criterion. |
| **Likelihood** | Measure between 0 and 1 of the possibility that an event will occur. |
| **Measures, preparatory** | Options for action during a crisis which are developed ahead of time. |
| **Measures, preventive** | Actions and means developed and used before a crisis occurs in order to reduce risks to the organization. These include measures to physically protect risk elements or to ensure the functionality of processes using redundant or substitute systems. Both aspects contribute to business continuity. |

[60] As defined by the Working Group on Infrastructure Protection (AK KRITIS) at the Federal Ministry of the Interior on 17 November 2003.

[61] Cf. von Rössing 2005, p. 428.

| Term | Definition |
|---|---|
| **Operating procedures** | Procedures for the workflow of an organizational unit, taking into account space, time, personnel and material resources. |
| **Organization** | Refers in this guide to all companies, public agencies and other institutions which operate a critical infrastructure. |
| **Organizational structure** | Divides an organization into static, primarily hierarchical units. |
| **Pandemic** | Cross-border or international outbreak of a disease. |
| **Plan-do-check-act (PDCA) cycle** | A process management tool for continuous improvement of the quality of these processes. “Plan” stands for comprehensive, overall planning of processes; “do” for the implementation of plans; “check” for checking the effectiveness of processes and “act” for the improvement of processes. This cycle is applied in risk and crisis management at various levels. |
| **Report** | Short and precise information on occurrences, perceptions and circumstances concerning a situation. |
| **Residual risks** | Risks remaining after preventive measures have been implemented.[62] |
| **Restart** | Phase following the completion of crisis response up to the start of business continuity operations.[63] |
| **Restoration** | Complete restoration of normal conditions as they existed before the crisis.[64] |
| **Risk** | Risk is viewed as a function of threat and the vulnerability of risk elements and sub-processes. The likelihood of an incident is one component of a threat analysis. |
| **Risk analysis** | A systematic procedure for identifying risk values.[65]<br>For the purposes of this guide, this includes<br>• an analysis of threats and exposure;<br>• an analysis of the vulnerability of all relevant sub-processes and risk elements;<br>• a comparison of sub-risks to individual risk elements and a comparison of scenario-related overall risks of sub-processes. |
| **Risk avoidance** | Strategic decisions that help remove threats or reduce their likelihood so that risks do not arise. |
| **Risk communications** | Risk management procedure for organizations to maintain and publish information on risks. Risk communications include all communication processes related to identifying, analysing, assessing and managing risks and the necessary interactions between those involved.[66] |

[62] Rössing 2005, p. 439.

[63] Rössing 2005, p. 439.

[64] Adapted from Australian/New Zealand Standard 2004, p. 3.

[65] Australian/New Zealand Standard 2004, p. 4.

[66] Jungermann et al. 1991, p. 5.

| Term | Definition |
|---|---|
| **Risk element** | Individual element of critical sub-processes. For the purposes of this guide, this includes<br>• people (staff and others on the premises)<br>• grounds<br>• buildings<br>• facilities and equipment<br>• special, organization-specific facilities and equipment<br>• data and files<br>• other resources |
| **Risk evaluation** | Procedure for relating the risk an incident poses for a sub-process or risk element to previously developed objectives in order to determine whether the risk and any residual risks are acceptable. |
| **Risk management** | A planning process or procedure to deal with risks. |
| **Risk reduction** | Measures to reduce the likelihood or impact of incidents on the organization. [67] |
| **Risk shifting** | Strategy of moving existing risks to other companies, authorities or insurance providers. |
| **Scenario** | Combination of assumptions on the possible sequence of events concerning the object currently under examination, in order to focus on causal connections and matters for decision. |
| **Single point of failure** | Process areas or individual risk elements whose disruption can lead to widespread failures or damage. |
| **Situation** | Type and extent of disruptions or damage and how they are likely to develop. |
| **Situation assessment** | Evaluation of disruptions or damage with regard to impacts and possible measures. |
| **Situation review** | The gathering, ordering, filing and representation of information about a situation. |
| **Strategic protection aims** | Description of desired objectives that can be used when evaluating measures implemented. |
| **Sub-risk** | Risk related to a risk element. |
| **Sub-vulnerability** | Vulnerability related to a risk element. |
| **Table top exercise** | Exercise involving only the members of the crisis task force and organization executive. |
| **Threat** | A cause of possible disruption.[68] |
| **Vulnerability** | The susceptibility of an object or system to threats. |
| **Vulnerability criterion** | Conditions for estimating vulnerability. |

[67] Australian/New Zealand Standard 2004, p. 5.

[68] Australian/New Zealand Standard 2004, p. 3.

# III. List of threats – Information on types, exposure, intensity, impacts and points of contact

**IMPORTANT NOTE:**
The list includes examples of threats which may affect the organization. Since it is not exhaustive, the list should be adapted to the specific circumstances of the examined sites, if needed.

| Type of threat | Exposure | Possible intensity | Possible impact | Responsibility, possible sources of Informationsquellen |
|---|---|---|---|---|
| Flood | Especially areas close to rivers and low areas, basements and ground floors | Large-scale flooding, water level up to several metres above the normal;<br>high flow velocity in low mountain ranges | Washouts, seepage (water damage) | Environmental agencies, flood centres, insurance companies |
| Storm/tornado | Across Germany | Very high winds | Pressure and suction effects on buildings and other items; destruction | Environmental agencies, German Meteorological Service |
| Earthquake | Places in earthquake zones (Rhine Rift, Cologne Bay, Vogtland, Swabian Alp) | Enormous horizontal and vertical forces; high energy input | Destruction of pipes, tanks, transformers, connections between facilities and buildings; debris | Federal Institute for Geosciences and Natural Resources |
| Wildfire | Densely wooded areas | Extreme heat | Threat to staff, destruction of facilities due to heat; power supply and IT systems are affected | Environmental agencies, German Meteorological Service, fire brigades, regulatory agencies |
| Drought | Especially dry regions with low rainfall | Long lack of rainfall, very low precipitation | Groundwater drawdown; lack of cooling and drinking water; power outages, problems in waterway transport | Operators, environmental agencies, German Meteorological Service |

| Type of threat | Exposure | Possible intensity | Possible impact | Responsibility, possible sources of Informationsquellen |
|---|---|---|---|---|
| Heatwave | Across Germany | High day and night temperatures | Impact on the health of staff and customers | Health agencies, German Meteorological Service |
| Large epidemic/ pandemic | Worldwide/ across Germany/ regional | High contamination rate, rapid spread, virulence of the virus | Staff and clients fall ill; staff are insecure (psychological effects such as panic); staff with sick relatives cannot work (care) | Health agencies, Robert Koch Institute, Federal Office for Civil Protection and Disaster Response |
| Failure of the external power supply | Across Germany; several days, over a large area |  | Damage to facilities and equipment | Suppliers, fire brigade, relief organizations |
| Failure of the external water supply | Across Germany |  | Impact on staff, damage to facilities and equipment | Suppliers, fire brigade, relief organizations |
| Failure of outsourced specialized services | Across Germany |  | Impact on staff and working materials | Regulatory agencies, transport authorities depending on the carrier |
| Accident involving dangerous goods within the facility or in its immediate vicinity | Near transport routes of hazardous goods (railway and road); near facilities in which hazardous goods are used | High concentration of the released agent; highly toxic effect of the released agent | Impact on staff, clients, buildings (contamination) | Environmental agencies, fire brigades, TUIS,[69] health offices |
| Attack with conventional explosives and incendiary devices | Across Germany | Extremely high local destructiveness | Impact on staff, clients, buildings and facilities; debris | Police, fire brigade |
| Attack with unconventional explosives and incendiary devices or release of NBC agents within the facility or in its immediate vicinity | Across Germany | High concentration of the released agent; higly toxic effect of the released agent | Impact on staff, clients, buildings and facilities (contamination) | Police, fire brigade |

[69] Since 1982 TUIS, a transport accident information and emergency response system, has provided assistance in transport and warehouse accidents involving chemical products across Germany. Some 130 chemical companies participate in TUIS by providing fire brigades and experts such as chemists, toxicologists and production experts. TUIS members are available via phone 24/7 to public services such as fire brigades, police and other authorities involved in crisis management as well as Deutsche Bahn and provide assistance using a three-level system.

| Type of threat | Exposure | Possible intensity | Possible impact | Responsibility, possible sources of Informationsquellen |
|---|---|---|---|---|
| Failure of information technology | Across Germany | High potential damage, rapid dissemination | Damage to facilities and equipment | German Federal Office for Information Security/threat registers[70] |
| Human error in connection with IT systems | Across Germany | High potential damage, rapid dissemination | Damage to facilities and equipment | German Federal Office for Information Security/threat registers[70] |
| Wilful acts using or against IT | Across Germany | High potential damage, rapid dissemination | Damage to facilities and equipment | German Federal Office for Information Security/threat registers[70] |
| Kidnapping | Across Germany | | Impact on staff | Police |
| Extortion | Across Germany | | Impact on staff or products | Police |
| Theft of critical facilities, devices and/or other equipment | Across Germany | | Possible damage to data, documents, facilities and equipment | Police |

[70] Federal Office for Information Security 2007.

# IV. Checklists

**IMPORTANT NOTE:**
The checklists should be adapted to the individual features of the facility. Using checklists is no substitute for setting up an extensive system of risk and crisis management. These lists are not exhaustive.

The checklists were compiled using the following references:

- American Water Works Association 2001
- British Standard 2006
- Federal Office for Civil Protection and Disaster Response 2005
- Federal Ministry of the Interior 2005
- Egli 1999
- Federal Emergency Management Agency 2003
- Gustin 2004
- Jungbluth 2005
- National Fire Protection Association 2004
- Federal Environmental Agency2005a
- Federal Environmental Agency 2005b
- Research Centre on Alpine Environment 2000

For more information see:

- Verwaltungs-Berufsgenossenschaft VBG 2007
- VdS Guidelines: Programme 2007

For further information on pandemic planning see:

- Federal Office for Civil Protection and Disaster Response 2007
- Department of Health and Human Services and the Centers for Disease Control and Prevention
- Department of Homeland Security 2006

## IV.1 Preventive measures

### IV.1.1 Risk and crisis management – general

| Questions | Notes | Yes | No | n/a | Comments |
|---|---|---|---|---|---|
| 1. Is risk management in place? | Planning, implementation, maintenance and constant improvement | ○ | ○ | ○ | |
| 2. Does the risk management follow specifically defined work processes? | | ○ | ○ | ○ | |
| 3. Were strategic protection aims defined? | | ○ | ○ | ○ | |
| 4. Is there an inventory of critical processes, are they categorized, and are there guidelines for performing these processes? | Inventory, criticality analysis, priorities of critical processes | ○ | ○ | ○ | |
| 5. Is crisis management in place? (incident management) | Reporting channels, reporting procedures, incident management, improvements | ○ | ○ | ○ | |
| 6. Are internal continuity plans and an internal continuity management in place? | Planning redundant and backup systems and their management in case of an incident | ○ | ○ | ○ | |
| 7. Is compliance with legal obligations monitored? | Compliance with legal obligations, guidelines and standards, system audit | ○ | ○ | ○ | |
| 8. Does staff development take security aspects into account? | Tasks and responsibilities, monitoring, training and awareness-raising | ○ | ○ | ○ | |
| | | | | | |

### IV.1.2 Grounds, buildings, facilities – floods

| Questions | Notes | Yes | No | n/a | Comments |
|---|---|---|---|---|---|
| **1. Buildings** | | | | | |
| 1.1 Can the flooding of planned or existing facilities be ruled out? | | ○ | ○ | ○ | |
| a) through floods | | ○ | ○ | ○ | |
| b) through backwater from the canal system | | ○ | ○ | ○ | |
| c) through rising groundwater | | ○ | ○ | ○ | |
| d) through water used in fire-fighting operations | | ○ | ○ | ○ | |
| 1.2 Have measures been taken to protect the facility against floods? | | ○ | ○ | ○ | |
| 1.3 Are new buildings planned to be elevated, if possible? | This refers to buildings and inlets. | ○ | ○ | ○ | |
| 1.4 Is the outer shell of the building flood-proof? | | ○ | ○ | ○ | |
| 1.5 Are inlets in the outer shell of the buildings flood-proof? | This includes temporary or mobile and permanent measures. | ○ | ○ | ○ | |
| 1.6 Are the furnishings and use of indoor space adapted to the possible threat of a flood? | For example by using water-proof building materials. | ○ | ○ | ○ | |
| 1.7 Would rising ground-water due to a flood impair building stability? | For example basements (floating effect) | ○ | ○ | ○ | |
| 1.8 Could the land on which buildings are located be affected by washouts? | | ○ | ○ | ○ | |

| Questions | Notes | Yes | No | n/a | Comments |
|---|---|---|---|---|---|
| **2. Facilities** | | | | | |
| 2.1 Are containers and pipes sufficiently anchored or secured against lifting? | This includes anchorage, the design of oil and diesel tanks taking into account hydrostatic pressure, the design of feed and drain pipes, tank venting and feed pipe to the burner. | ○ | ○ | ○ | |
| 2.2 Are containers and pipes sufficiently anchored or secured against mechanical damage caused by floating debris? | This includes anchorage, the design of oil and diesel tanks taking into account hydrostatic pressure, the design of feed and drain pipes, tank venting and feed pipe to the burner. | ○ | ○ | ○ | |
| 2.3 Has a backwater protection been installed in the canalization? | | ○ | ○ | ○ | |

### IV.1.3 Grounds, buildings, facilities – earthquakes

| Questions | Notes | Yes | No | n/a | Comments |
|---|---|---|---|---|---|
| **1. Buildings** | | | | | |
| 1.1 Can buildings sufficiently withstand earthquakes? | This includes adhering to standards (DIN 4149, Eurocode 8) and voluntarily applying recommendations going beyond these standards. | ○ | ○ | ○ | |
| 1.2 Are facilities within the building sufficiently anchored? | This includes tanks, transformers etc. | ○ | ○ | ○ | |
| 1.3 Can changes weakening the structure of supporting elements be ruled out? | This includes large drill holes and supplementary cut-outs. | ○ | ○ | ○ | |

| Questions | Notes | Yes | No | n/a | Comments |
|---|---|---|---|---|---|
| **2. Underground facilities** | | | | | |
| 2.1 Is the potential burden taken into account when laying pipes in earthquake areas? | This includes soil conditions, laying the pipes at a right angle to known faults with flexible joints and relief valves, and laying redundant pipes. | ○ | ○ | ○ | |

### IV.1.4 Grounds, buildings – storms

| Questions | Notes | Yes | No | n/a | Comments |
|---|---|---|---|---|---|
| **1. Roofs** | | | | | |
| 1.1 Are roofs sufficiently anchored to the buildings? | | ○ | ○ | ○ | |

### IV.1.5 Grounds, buildings – wilful criminal and/or terrorist acts

| Questions | Notes | Yes | No | n/a | Comments |
|---|---|---|---|---|---|
| **1. Access** | | | | | |
| 1.1 Is access to the organization's grounds controlled? | | ○ | ○ | ○ | |
| 1.2 Are there restricted access zones on the organization's grounds? | An important measure to prevent terrorist attacks or sabotage is to create a distance between the buildings and possible car bombings. Barriers and obstacles that can be used to create a distance such as different elevations, bollards, fences or concrete barriers may prevent vehicles from approaching critical areas. | ○ | ○ | ○ | |
| | | | | | |

| Questions | Notes | Yes | No | n/a | Comments |
|---|---|---|---|---|---|
| 1.3 Are there restricted access areas in the buildings? | It should be examined whether single-entry access control systems can be installed, possibly combined with card readers, to control access and restrict access for non-employees. | ○ | ○ | ○ | |
| 1.4 Are access controls carried out in the buildings? | For example by the doorman. | ○ | ○ | ○ | |
| 1.5 Are critical areas locked and accessible only to authorized staff? | | ○ | ○ | ○ | |
| **2. Construction** | | | | | |
| 2.1 Are the facades, including windows and doors, reinforced? | Doors and windows should incorporate laminated safety glass. | ○ | ○ | ○ | |
| 2.2 Are there protected areas for staff and other persons? | As a precaution against terrorist attacks, incidents involving dangerous goods, or industrial disasters it may be useful to integrate protected areas where staff and visitors can take shelter. This may be done using static support cores such as staircases and areas of the lower floors equipped with smoke barrier doors and communication systems. On the basis of existing plans it should be examined whether protected areas can be established. | ○ | ○ | ○ | |
| 2.3 Are air inlets difficult to reach from outside? | This means, that they are located in sufficiently high or inaccessible places. | ○ | ○ | ○ | |

| Questions | Notes | Yes | No | n/a | Comments |
|---|---|---|---|---|---|
| **3. Electronic surveillance** | | | | | |
| 3.1 Are critical areas monitored by video cameras? | | ○ | ○ | ○ | |
| 3.2 Are video recordings evaluated? | | ○ | ○ | ○ | |
| 3.3 Are alarm systems installed in core areas? | | ○ | ○ | ○ | |
| **4. Contact persons** | | | | | |
| 4.1 Are there specialized contact persons who may be contacted in case of an attack using chemical, biological or radiological agents? | In case of an accident or attack public and private bodies may have to deal with agents whose assessment requires expert knowledge. In addition to health agencies, possible partners should be identified and contacted in advance. | ○ | ○ | ○ | |

**IV.1.6 Facilities and equipment – power supply**

| Questions | Notes | Yes | No | n/a | Comments |
|---|---|---|---|---|---|
| **1. Power supply** | | | | | |
| 1.1 Are there several power feeds, and do they belong to independent grids? | | ○ | ○ | ○ | |
| **2. Backup power supply** | | | | | |
| 2.1 Have critical areas been identified which need backup power supply in case of crisis? | Critical areas include control centres, data centres, and air conditioning systems in data centres. | ○ | ○ | ○ | |

| Questions | Notes | Yes | No | n/a | Comments |
|---|---|---|---|---|---|
| 2.2 Have precautions been taken to ensure that only those consumers required for emergency operation in critical areas are connected to the backup power supply? | | ○ | ○ | ○ | |
| 2.3 Is there a defined period of time during which critical areas will remain connected to the backup power supply? | | ○ | ○ | ○ | |
| 2.4 Has the total amount of energy required to maintain critical areas been identified? | | ○ | ○ | ○ | |
| 2.5 Do backup generators meet the current capacity and quality requirements? | Capacity and quality requirements change when new, modern facilities are developed. | ○ | ○ | ○ | |
| 2.6 Is there sufficient fuel for the defined operation period of the backup power supply? | | ○ | ○ | ○ | |
| 2.7 Are all backup generators regularly maintained? | | ○ | ○ | ○ | |
| 2.8 Are all backup generators regularly tested under full load? | | ○ | ○ | ○ | |
| 2.9 Can backup generators be put into operation without any difficulty in crisis situations? | A starting aid such as the power supply or batteries may fail in crisis situations. Equipment often needs to be warmed up. | ○ | ○ | ○ | |
| 2.10 Is information communicated if a backup generator needs refuelling? | How and where? | ○ | ○ | ○ | |
| 2.11 Are sensitive technical components protected by an uninterruptible power supply? | This includes a battery buffer which provides IT systems with energy for a few minutes. | ○ | ○ | ○ | |

| Questions | Notes | Yes | No | n/a | Comments |
|---|---|---|---|---|---|
| 2.12 Have you concluded agreements or contracts with providers of resources for backup generators? | | ○ | ○ | ○ | |
| **3. Security and warning systems which do not depend on power supply** | | | | | |
| 3.1 Has emergency lighting been installed which is independent of public power supply? | Emergency lighting is independent of public power supply if it is run by a battery, for example. | ○ | ○ | ○ | |
| 3.2 Has an alarm and warning system been installed which is independent of power supply? | An alarm and warning system is independent of public power supply if it is run by a battery, for example. | ○ | ○ | ○ | |

### IV.1.7 Facilities and equipment – information technology

| Questions | Notes | Yes | No | n/a | Comments |
|---|---|---|---|---|---|
| **1. General** | | | | | |
| 1.1 Is efficient IT management in place? (procurement, development and maintenance of information systems) | System security requirements, correct processing in applications, cryptographic measures, security of system files and processes, vulnerability management | ○ | ○ | ○ | |
| **2. Access control** | | | | | |
| 2.1 Is IT connected to public data networks sufficiently protected against external access? | | ○ | ○ | ○ | |
| **3. Backup** | | | | | |
| 3.1 Is there a data backup plan? | | ○ | ○ | ○ | |
| 3.2 Are critical data stored in different places? | | ○ | ○ | ○ | |

| Questions | Notes | Yes | No | n/a | Comments |
|---|---|---|---|---|---|
| **4. Process control** | | | | | |
| 4.1 Is there a redundant, physically separate system of process control? | | ○ | ○ | ○ | |
| 4.2 Are process control and security systems (alarm system, video surveillance etc.) separate (separate networks)? | If process control is performed while being connected to the Internet and process control and security systems are connected as well, both systems may be manipulated from outside. | ○ | ○ | ○ | |

### IV.1.8 Facilities and equipment – communications technology

| Questions | Notes | Yes | No | n/a | Comments |
|---|---|---|---|---|---|
| **1. Landline** | | | | | |
| 1.1 Is the telephone system protected by an uninterruptible power supply? | | ○ | ○ | ○ | |
| 1.2 Is the telephone system also protected by a backup generator? | | ○ | ○ | ○ | |
| 1.3 Has priority network access been requested? | | ○ | ○ | ○ | |
| **2. Mobile phones** | | | | | |
| 2.1 Are staff equipped with mobile phones for crisis situations? | | ○ | ○ | ○ | |
| **3. Radio** | | | | | |
| 3.1 Does the company have a radio communications system? | | ○ | ○ | ○ | |

## IV.2 Crisis management review

### IV.2.1 General organization

| Questions | Notes | Yes | No | n/a | Comments |
|---|---|---|---|---|---|
| **1. Responsibilities and tasks** | | | | | |
| 1.1 Is there a staffing scheme for the required crisis management positions at the facility? | | ○ | ○ | ○ | |
| 1.2 Are all relevant crisis management tasks defined and assigned to staff and their deputies? | | ○ | ○ | ○ | |
| 1.3 Are staff trained for their assigned roles during crisis? | | ○ | ○ | ○ | |
| **2. Alerts** | | | | | |
| 2.1 Are internal and external alert and information processes clearly defined? | | ○ | ○ | ○ | |
| 2.2 Are there specific instructions for persons who are responsible for passing on information during a crisis? | | ○ | ○ | ○ | |
| 2.3 Are actions and decisions during a crisis recorded? | | ○ | ○ | ○ | |
| 2.4 Are there exercises to practise internal and external alert and information processes? | This includes internal exercises and participation in local emergency exercises | ○ | ○ | ○ | |
| | | | | | |

| Questions | Notes | Yes | No | n/a | Comments |
|---|---|---|---|---|---|
| **3. Alerts** | | | | | |
| 3.1 Is the alert adapted to possible impacts of major emergencies? | Simplified definition based on the following criteria, e. g.:<br>1) Only one part of the organization is affected.<br>2) The whole organization is affected but impacts do not extend beyond the organization.<br>3) The whole facility and its surroundings/region are affected.<br>4) The whole organization, its surroundings and areas beyond the organization's immediate vicinity are affected. | ○ | ○ | ○ | |
| **4. Warning** | | | | | |
| 4.1 Is there a warning scheme to inform the population affected by an extreme event in the organization? | Residents, clients, etc. | ○ | ○ | ○ | |
| **5. Task forces** | | | | | |
| 5.1 Is a task force convened in case of crisis at the organization? | | ○ | ○ | ○ | |
| 5.2 Does the organization appoint liaison officers to crisis task forces (operations command, administrative staff)? | In the event of a crisis, the organization will have more influence on decisions affecting it if liaison officers are represented in these task forces. Contact the local civil protection authorities, including fire brigades and local and regional administrations. | ○ | ○ | ○ | |
| | | | | | |

| Questions | Notes | Yes | No | n/a | Comments |
|---|---|---|---|---|---|
| 5.3 Are there areas which the task force may use during crisis and which provide the necessary technical equipment and backup power supply? | | ○ | ○ | ○ | |
| 5.4 Are there strategies on how the task force may continue its work if communication systems break down? | For example by using proximity detectors with or without cars or motorcycles. | ○ | ○ | ○ | |
| 5.5 Are there strategies on how the task force may continue its work if data processing systems break down? | For example by keeping hard copies of plans and information. | ○ | ○ | ○ | |
| 5.6 Are there strategies on how the task force may continue its work if the crisis management centre can no longer be used? | | ○ | ○ | ○ | |
| **6. Required information and files** | | | | | |
| 6.1 Are there floor plans of the buildings, plans of the position of supply and return lines and of access routes in digital and printed form? | Supply and return lines include electricity, gas and water. | ○ | ○ | ○ | |
| 6.2 Do the floor plans include and mark all information necessary in a crisis? | This includes escape routes, emergency exits, staircases, fire extinguishers, first-aid kits, secure retreats, storage rooms, equipment rooms, backup power generators, assembly areas, pipes, valves, slides, etc. | ○ | ○ | ○ | |
| 6.3 Are all necessary files within reach? | For example: contracts | ○ | ○ | ○ | |

| Questions | Notes | Yes | No | n/a | Comments |
|---|---|---|---|---|---|
| 6.4 Are there waterproof plans and files which could be also used outdoors during a crisis? | | ○ | ○ | ○ | |
| 6.5 Are there forms to record incoming and outgoing information? | | ○ | ○ | ○ | |
| 6.6 Are there forms to compile information to be communicated to the public? | | ○ | ○ | ○ | |
| **7. Contact information** | | | | | |
| 7.1 Are there up-to-date, centrally maintained lists of staff and contact information? | The lists include names, addresses, telephone numbers (private and office), and a description of the position in the organization. | ○ | ○ | ○ | |
| 7.2 Are there up-to-date lists of information about important external companies and authorities? | The lists include information on the organization, the address, the name of a contact person, a description of services, and information on contracts and supply priorities. This includes hospitals, kindergartens, schools and suppliers of raw and working materials. | ○ | ○ | ○ | |
| 7.3 Are all lists regularly updated? | | ○ | ○ | ○ | |
| **8. Possible coordination with responsible authorities** | | | | | |
| 8.1 Does the contingency plan list the authorities to be notified? | Examples: Police, health agency, environmental agency, fire brigade, civil protection agency | ○ | ○ | ○ | |
| 8.2 Do these authorities know who is responsible for what in the organization? | | ○ | ○ | ○ | |
| | | | | | |

| Questions | Notes | Yes | No | n/a | Comments |
|---|---|---|---|---|---|
| 8.3 Are the responsible authorities informed about contingency plans? | | ○ | ○ | ○ | |
| 8.4 Is the organization in contact with police authorities responsible for threat prevention? | These authorities (Federal Police and Land police, Land Criminal Police Offices, Federal Criminal Police Office) advise on questions in connection with events of criminal or terrorist background or sabotage. | ○ | ○ | ○ | |

**IV.2.2 Staff – general**

| Questions | Notes | Yes | No | n/a | Comments |
|---|---|---|---|---|---|
| 1. Are there strategies and measures to protect staff also during extreme situations? | This includes training staff to become evacuation wardens and first aiders, and to assist during pandemics, evacuation plans, escape routes free of flooding and debris, retreats, shelters, first-aid equipment and food supplies. | ○ | ○ | ○ | |
| 2. Do staff working at the organization have sufficient local knowledge? | | ○ | ○ | ○ | |
| 3. Have staff worked in different areas of the organization (rotation principle)? | Rotating through different tasks allows staff to work outside their usual sphere of responsibility if the responsible staff are not able to perform these tasks. | ○ | ○ | ○ | |
| 4. Are there substitute staff for emergencies? | During pandemics, for example, staff from neighbouring companies and authorities, retired staff or trainees may be used. | ○ | ○ | ○ | |
| | | | | | |

| Questions | Notes | Yes | No | n/a | Comments |
|---|---|---|---|---|---|
| 5. Are there alert strategies for single-person workplaces? | This includes alarm buttons and an automated alarm in case of malfunctions, mistakes and missing corrections in control centres. | ○ | ○ | ○ | |
| 6. Are staff informed about the facility's crisis management? | | ○ | ○ | ○ | |

### IV.2.3 Crisis management – pandemic planning (especially influenza pandemic)

| Questions | Notes | Yes | No | n/a | Comments |
|---|---|---|---|---|---|
| **1. General** | | | | | |
| 1.1 Have precautions been taken to gradually shut down operations within the organization if there is a serious lack of staff? | | ○ | ○ | ○ | |
| 1.2 Are there alternative work places which can be used during an epidemic or pandemic? | For example: telework | ○ | ○ | ○ | |
| 1.3 Have agreements been concluded on shifting tasks to external service providers? | | ○ | ○ | ○ | |
| 1.4 Does the organization cooperate with local health authorities in the framework of preliminary planning? | | ○ | ○ | ○ | |
| 1.5 Does the organization maintain a supply of antiviral medicines? | | ○ | ○ | ○ | |
| 1.6 Does the organization offer vaccination or does it inform about vaccination possibilities? | | ○ | ○ | ○ | |

| Questions | Notes | Yes | No | n/a | Comments |
|---|---|---|---|---|---|
| 1.7 Can the air conditioning be partly switched off if needed? | It needs to be taken into account that certain areas and equipment require constant air conditioning, e. g. server rooms. Such rooms and equipment require separate air conditioning. | ○ | ○ | ○ | |
| **2. Staff** | | | | | |
| 2.1 Are staff made aware of the issue? | | ○ | ○ | ○ | |
| 2.2 Are staff trained on how to behave during an incident? | Examples:<br>■ Avoid touching face with hands;<br>■ Avoid shaking hands<br>■ Regularly wash hands<br>■ Wear equipment for personal protection (mouth and nose mask, safety glasses) | ○ | ○ | ○ | |
| 2.3 Have critical staff been identified? | | ○ | ○ | ○ | |
| 2.4 Have critical staff been informed about isolation during an incident? | | ○ | ○ | ○ | |
| 2.5 Are additional staff trained for specific operations within the organization? | | ○ | ○ | ○ | |

## IV.3 Crisis management

### IV.3.1 General procedures during crisis

| Questions | Notes | Yes | No | n/a | Comments |
|---|---|---|---|---|---|
| **1. General procedures** | | | | | |
| 1.1 Has the situation been analysed? | | ○ | ○ | ○ | |
| 1.2 Can operations be restored? | | ○ | ○ | ○ | |
| 1.3 Are precautions taken for staff, visitors and clients? | | ○ | ○ | ○ | |
| 1.4 Are precautions taken for buildings, equipment, data and files? | | ○ | ○ | ○ | |
| **2. Administrative procedures** | | | | | |
| 2.1 Are staff, visitors and clients warned when a serious incident occurs? | | ○ | ○ | ○ | |
| 2.2 Are all staff involved in crisis management identified? | | ○ | ○ | ○ | |
| 2.3 Are all staff working in hazard zones identified? | | ○ | ○ | ○ | |
| 2.4 Is help provided to injured, stranded or lost staff? | | ○ | ○ | ○ | |
| 2.5 Are staff informed about the incident? | | ○ | ○ | ○ | |
| 2.6 Are the staff's families informed about the incident? | | ○ | ○ | ○ | |
| 2.7 Are all injuries and the related measures taken recorded? | | ○ | ○ | ○ | |

| Questions | Notes | Yes | No | n/a | Comments |
|---|---|---|---|---|---|
| 2.8 Are all sub-events recorded? | | ○ | ○ | ○ | |
| 2.9 Are all facilities and equipment removed from damage zones? | | ○ | ○ | ○ | |
| 2.10 Is access to the damage zone controlled? | | ○ | ○ | ○ | |
| 2.11 Are minutes taken of all telephone calls? | | ○ | ○ | ○ | |
| 2.12 Are press releases published? | | ○ | ○ | ○ | |
| 2.13 Is the alert cancelled and are operations restored after the crisis has ended? | | ○ | ○ | ○ | |
| **3. Logistics** | | | | | |
| 3.1 Is the necessary equipment provided? | | ○ | ○ | ○ | |
| 3.2 Are food and daily tools provided? | | ○ | ○ | ○ | |
| 3.3 Is the crisis management centre operational? | | ○ | ○ | ○ | |
| 3.4 Are the necessary plans provided? | Plan of the building, power supply, water supply, sewage, etc. | ○ | ○ | ○ | |
| 3.5 Are all redundant facilities and equipment provided? | Alternative crisis management centre, radio equipment, etc. | ○ | ○ | ○ | |
| 3.6 Is damaged equipment repaired or is repair initiated? | | ○ | ○ | ○ | |
| 3.7 Is medical assistance provided for possible injured persons? | | ○ | ○ | ○ | |
| 3.8 Is the backup power supply switched on? | | ○ | ○ | ○ | |

### IV.3.2 Special emergency procedures

| Questions | Notes | Yes | No | n/a | Comments |
|---|---|---|---|---|---|
| **1. Rescue, retrieve, extinguish** | | | | | |
| 1.1 Are all necessary steps taken to rescue persons and retrieve equipment? | Informing external bodies | ○ | ○ | ○ | |
| 1.2 Are all necessary steps taken to extinguish fires? | Internal measures; informing external bodies | ○ | ○ | ○ | |
| **2. Medical first aid** | | | | | |
| 2.1 Are all necessary steps taken to provide first aid? | Internal measures; informing external bodies | ○ | ○ | ○ | |
| 2.2 Are all necessary external bodies alerted to provide first aid? | Rescue service, fire brigade, etc. | ○ | ○ | ○ | |
| **3. Barriers and access controls** | | | | | |
| 3.1 Are all necessary measures taken to seal off the organization? | | ○ | ○ | ○ | |
| 3.2 Is access to emergency zones controlled? | | ○ | ○ | ○ | |
| **4. Safe accommodation** | | | | | |
| 4.1 Is safe accommodation provided to task force members? | Areas where they can stay during the day and sleep at night, if needed. | ○ | ○ | ○ | |
| 4.2 Is safe accommodation provided to staff, visitors and clients? | Areas where they can stay during the day and sleep at night, if needed. | ○ | ○ | ○ | |
| | | | | | |

| Questions | Notes | Yes | No | n/a | Comments |
|---|---|---|---|---|---|
| **5. Evacuation of buildings** | | | | | |
| 5.1 Are all persons present led to the determined assembly areas by evacuation wardens? | | ○ | ○ | ○ | |
| 5.2 Is a head count taken at the assembly area? | | ○ | ○ | ○ | |
| 5.3 Is it announced when the evacuation is completed? | | ○ | ○ | ○ | |
| 5.4 Are means of transport provided to take the persons present to another place? | | ○ | ○ | ○ | |
| **6. Response to a bomb threat** | | | | | |
| 6.1 Are the police informed? | | ○ | ○ | ○ | |
| 6.2 Is information about suspicious activities recorded and passed on? | | ○ | ○ | ○ | |
| 6.3 Is information about suspicious items recorded and passed on? | (e. g. by using a form) | ○ | ○ | ○ | |
| **7. Coordinating cooperation with external companies and authorities** | | | | | |
| 7.1 Has the procedure for cooperation with external companies and authorities been activated? | For example: fire brigade, police | ○ | ○ | ○ | |
| 7.2 Is access of staff from external organizations controlled? | | ○ | ○ | ○ | |
| 7.3 Are necessary communication channels activated? | | ○ | ○ | ○ | |

| Questions | Notes | Yes | No | n/a | Comments |
|---|---|---|---|---|---|
| **8. Controlled shut-down and start-up of operations** | | | | | |
| 8.1 Is the organization completely or partly shut down in consultation with the head of the task force? | | ○ | ○ | ○ | |
| 8.1 Are all time limits observed? | Possible lead times | ○ | ○ | ○ | |
| 8.1 Are the impacts of a partial or complete shut-down of facilities recorded and taken into account? | | ○ | ○ | ○ | |
| **9. Handling of critical data and files** | | | | | |
| 9.1 Are important storage media and files always kept in water- and fireproof containers? | | ○ | ○ | ○ | |
| 9.2 Are important storage media, files and containers labelled? | | ○ | ○ | ○ | |
| 9.3 Are important storage media and files removed from the damage zone? | | ○ | ○ | ○ | |
| **10. Media** | | | | | |
| 10.1 Are all trained media spokespersons called up? | | ○ | ○ | ○ | |
| 10.2 Are all prepared texts within reach? | | ○ | ○ | ○ | |
| 10.3 Is background material on the facility available? | | ○ | ○ | ○ | |

| Questions | Notes | Yes | No | n/a | Comments |
|---|---|---|---|---|---|
| 10.4 Is the required procedure for disclosing information to the public adhered to? | | ○ | ○ | ○ | |
| 10.5 Are all contact lists available to media representatives? | | ○ | ○ | ○ | |
| 10.6 Is there a questionnaire for checking media representatives? | authenticity, checking identity documents | ○ | ○ | ○ | |
| 10.7 Are all media representatives treated equally? | | ○ | ○ | ○ | |
| 10.8 Media<br>a. Are press releases published?<br>b. Are press conferences held?<br>c. Are informational announcements published?<br>d. Is information distributed via radio and TV? | | ○ | ○ | ○ | |

### 11. Financial support in a crisis

| Questions | Notes | Yes | No | n/a | Comments |
|---|---|---|---|---|---|
| 11.1 Are all required resources to cope with a crisis provided? | | ○ | ○ | ○ | |

### 12. Keeping records/securing evidence

| Questions | Notes | Yes | No | n/a | Comments |
|---|---|---|---|---|---|
| 12.1 Are all decisions recorded? | forms, minutes | ○ | ○ | ○ | |
| 12.2 Are all personal damages recorded? | reports, photos, videos | ○ | ○ | ○ | |
| 12.3 Is all material damage recorded? | reports, photos, videos | ○ | ○ | ○ | |

### IV.4 Follow-up

| Questions | Notes | Yes | No | n/a | Comments |
|---|---|---|---|---|---|
| 1. Are priorities established? | | ○ | ○ | ○ | |
| 2. Is the residual threat level identified? | | ○ | ○ | ○ | |
| 3. Will a survey on crisis management be conducted among staff? | | ○ | ○ | ○ | |
| 4. Will information on damage be evaluated? | reports, photos, videos | ○ | ○ | ○ | |
| 5. Are all bills settled? | | ○ | ○ | ○ | |
| 6. Are external organizations informed about the current situation? | insurance companies, authorities | ○ | ○ | ○ | |
| 7. Have clients concerned been contacted? | | ○ | ○ | ○ | |
| 8. Has the necessary clean-up work been initiated? | airing, removing debris, drying, etc. | ○ | ○ | ○ | |
| 9. Is an inventory of the damaged buildings, facilities and equipment being taken? | | ○ | ○ | ○ | |
| 10. Is the financial damage estimated? | | ○ | ○ | ○ | |
| 11. Will the results of the follow-up be used to adapt crisis management? | | ○ | ○ | ○ | |

## IV.5 Exercises

| Questions | Notes | Yes | No | n/a | Comments |
|---|---|---|---|---|---|
| **1. Table-top exercises** | | | | | |
| 1.1 Are emergency tasks and responsibilities practiced in exercises? | | ○ | ○ | ○ | |
| 1.2 Are alert, warning and reporting procedures exercised? | | ○ | ○ | ○ | |
| 1.3 Are internal and external communication channels tested? | | ○ | ○ | ○ | |
| 1.4 Are means of communication tested? | | ○ | ○ | ○ | |
| 1.5 Are contact lists tested? | For example: telephone lists | ○ | ○ | ○ | |
| **2. Partial and full-scale exercises** | | | | | |
| 2.1 Are buildings evacuated? | | ○ | ○ | ○ | |
| 2.2 Is a head count taken after evacuation? | | ○ | ○ | ○ | |
| 2.3 Is all equipment tested? | For example: personal protection equipment | ○ | ○ | ○ | |
| 2.4 Is a controlled shut-down of systems and areas practiced? | | ○ | ○ | ○ | |
| 2.5 Is the activation of alternate sites and equipment tested? | | ○ | ○ | ○ | |
| 2.6 Is the activation of the emergency operation of redundant systems tested? | | ○ | ○ | ○ | |
| 2.7 Is the restoration of regular operations practiced? | | ○ | ○ | ○ | |

## IV.6 Selecting and equipping a crisis management centre

| Questions | Notes | Yes | No | n/a | Comments |
|---|---|---|---|---|---|
| **1. Layout** | | | | | |
| 1.1 Is the crisis management centre located in a protected area in the organization or at an alternate site? | | ○ | ○ | ○ | |
| 1.2 Is the crisis management centre centrally accessible? | | ○ | ○ | ○ | |
| 1.3 Are task force members/functions directly available? | | ○ | ○ | ○ | |
| 1.4 Is there enough parking space in the immediate vicinity? | | ○ | ○ | ○ | |
| 1.5 Is there a sufficiently large and separate meeting room (without phones) for briefings? | | ○ | ○ | ○ | |
| 1.6 Are there additional small meeting rooms for working groups and more detailed discussions? | | ○ | ○ | ○ | |
| 1.7 Is there enough workspace for the task force and auxiliary functions? | | ○ | ○ | ○ | |
| 1.8 Are windows screened from view, and is the crisis management centre protected against electronic eavesdropping? | | ○ | ○ | ○ | |
| 1.9 Are there retreat rooms/rest areas and eating areas, where staff could also sleep? | | ○ | ○ | ○ | |

| Questions | Notes | Yes | No | n/a | Comments |
|---|---|---|---|---|---|
| 1.10 Can rooms be darkened for presentations? | | ○ | ○ | ○ | |

## 2. Technical infrastructure

| Questions | Notes | Yes | No | n/a | Comments |
|---|---|---|---|---|---|
| 2.1 Are computers with Internet access, e-mail applications and external storage media for data transport available? | CD-ROM, external hard drives, USB sticks | ○ | ○ | ○ | |
| 2.2 Are laptops/notebooks and PDAs available? | | ○ | ○ | ○ | |
| 2.3 Is there a shared e-mail inbox with controlled distribution? | | ○ | ○ | ○ | |
| 2.4 Are there mobile phones with battery chargers and analogue telephones for which no power supply is needed? | | ○ | ○ | ○ | |
| 2.5 Is there a direct line to important companies and authorities? | | ○ | ○ | ○ | |
| 2.6 Is there a sufficient number of fax machines or PC fax servers? | | ○ | ○ | ○ | |
| 2.7 Are scanners available? | To scan documents, images, etc. | ○ | ○ | ○ | |
| 2.8 Can the company's video surveillance system be accessed? | | ○ | ○ | ○ | |
| 2.9 Can the company's information systems be accessed? | | ○ | ○ | ○ | |
| 2.10 Can the company's radio and radio technology be accessed? | | ○ | ○ | ○ | |

| Questions | Notes | Yes | No | n/a | Comments |
|---|---|---|---|---|---|
| 2.11 Is visualization technology available? | For example: screen, multimedia projector, flip chart, white board | ○ | ○ | ○ | |
| 2.12 Is there a sufficient number of TV sets, radios and VCRs? | To follow, analyse and record TV programmes and news coverage. | ○ | ○ | ○ | |
| 2.13 Are recordings available in playable formats? | | ○ | ○ | ○ | |
| 2.14 Is there a photocopier? | | ○ | ○ | ○ | |
| 2.15 Are cameras available? | | ○ | ○ | ○ | |
| 2.16 Is an uninterruptible power supply or backup power system available? | | ○ | ○ | ○ | |
| **3. Miscellaneous** | | | | | |
| 3.1 Have forms, protocol forms and templates been prepared? | | ○ | ○ | ○ | |
| 3.2 Are briefing forms available? | | ○ | ○ | ○ | |
| 3.3 Are telephone and contact lists as well as lists of resources available? | staff, equipment, provisions, emergency services, contracts in digital form and on paper | ○ | ○ | ○ | |
| 3.4 Are there lists of participants for briefings? | | ○ | ○ | ○ | |
| 3.5 Is there a seating plan for the task force? | | ○ | ○ | ○ | |
| 3.6 Are up-to-date plans and pictures of the facility available? | | ○ | ○ | ○ | |
| 3.7 Are there name tags/plates indicating the task force members' functions? | Possibly, place cards (indicating the area of responsibility) if the composition of the task force changes | ○ | ○ | ○ | |

| Questions | Notes | Yes | No | n/a | Comments |
|---|---|---|---|---|---|
| 3.8 Are there sufficient office supplies? | paper, pens, etc. | ○ | ○ | ○ | |
| 3.9 Is there a press centre with the necessary equipment such as TV and radio? | For bigger companies and authorities | ○ | ○ | ○ | |
| 3.10 Have access controls been established to enter the crisis management centre? | | ○ | ○ | ○ | |
| 3.11 Are personal, office and company ID cards checked? | | ○ | ○ | ○ | |
| 3.12 Are business cards available? | For example for media representatives | ○ | ○ | ○ | |
| 3.13 Is the provision of food ensured in case of an incident? | | ○ | ○ | ○ | |
| 3.14 Is protective equipment available for all staff? | safety glasses, helmets, safety shoes, protective masks and suits | ○ | ○ | ○ | |

# V. Risk analysis example

The following example of a fictitious organization shows how a risk analysis can be implemented in practice. The example will focus on examining the sub-process of a control room. The control room process will not be divided into further sub-processes.

A risk table created with a spreadsheet programme is used to conduct the risk analysis for the control room.

**V.1 Criticality analysis**

To identify the control room's criticality, two out of the four criteria described in Chapter 3.2.1 are used and assessed on the basis of the following categorization. The categorization should be understood as a suggestion which can be adapted to the organization's specific needs. The categories in bold frames were chosen for the control room sub-process.

**a) Time frame :**
**If the process is disrupted, how long will it take to have an impact on the organization's overall product/service?**

| Categories | Time until service or production is disrupted | Verbal categories |
|---|---|---|
| 1 | very short period (e. g. seconds or minutes) | sub-process is highly critical |
| 2 | short period (e. g. hours) | sub-process is critical |
| 3 | medium period (e. g. days) | sub-process is important but not critical |
| 4 | long period (e. g. weeks) | sub-process is not very critical |
| 5 | very long period (e. g. months, years) | sub-process is almost uncritical |

Table 1: Categorization of the criticality criterion "time frame"

**b) Magnitude:**
**How much of the overall product/service will be affected if this process is interrupted or completely stopped?**

| Categories | Magnitude of disruption of the service or production | Verbal categories |
|---|---|---|
| 1 | very high (e. g. 80 to 100 % of the overall service or production) | sub-process is highly critical |
| 2 | high<br>(e. g. 50 to 80 % of the overall service or production) | sub-process is critical |
| 3 | medium<br>(e. g. 30 to 50 % of the overall service or production) | sub-process is important but not critical |
| 4 | low<br>(e. g. 10 to 30 % of the overall service or production) | sub-process is not very critical |
| 5 | very low<br>(e. g. 0 to 10 % of the overall service or production) | sub-process is almost uncritical |

Table 2: Categorization of the criticality criterion "magnitude"

The time until the entire service of the fictitious organization is disrupted is very short and can be assigned to the first category. Regarding the criterion "time frame" the sub-process is therefore highly critical.

It can be assumed that the magnitude of the organization's disrupted services is very high if the control room is affected; it can therefore be assigned to the second category. Regarding the criterion "magnitude" the sub-process is therefore critical.

The overall sub-process "control room" is considered highly critical and will be further examined in the framework of the risk analysis.

### V.2 Threat analysis and scenario development

A possible threat to the fictitious organization is for example a power blackout. This might create the following scenario.

**Scenario: Blackout**

| | |
|---|---|
| Intensity | 5 million people across Europe without electricity<br>All electrical systems of the organization without backup power supply fail.<br>The backup generators of crisis management authorities are not able to meet the demand for external backup power supply. |
| Geographical dimension | Regional outages in many regional sub-grids; the organization's control room is affected by the blackout. |
| Duration | 4 days |
| Warning | No warning |
| Reference incidents | Blackout in Münsterland in November 2005 with regional outages of up to five days affecting some 250,000 people |

Table 3: Scenario – Breakdown of the external power supply

It is almost impossible to determine the probability of this scenario in quantitative terms. Therefore, it must be estimated. The recent past has shown that short-term blackouts do occur. Given an increase in extreme natural events and the growing threat posed by terrorist attacks, the likelihood of this scenario is classified as moderate. This corresponds to category no. 3.

**Question: How would you estimate the probability that such a scenario will occur in the scope described?**

| Categories | Verbal categories | Points |
|---|---|---|
| 1 | very low | 1 |
| 2 | low | 2 |
| 3 | medium | 3 |
| 4 | high | 4 |
| 5 | very high | 5 |

Table 4: Probability categories

### V.3 Vulnerability analysis

The following vulnerability criteria from Chapter 3.2.2.2 are selected for the control room:

- Dependence on risk elements
- Dependence on external infrastructures – power supply
- Dependence on external infrastructures – traffic, transport and logistics
- Robustness/actual level of protection
- Redundancy, substitutes
- Restoration effort

It is assumed that these criteria are particularly relevant for the fictitious organization. In order to simplify the example, no reasons are given this selection, but it shows that not all vulnerability criteria need to be selected for all facilities.

The criterion "dependence on risk elements" serves as a quantifier; the sum of the remaining values is used for risk calculation.

Just as when estimating a scenario's likelihood, the risk elements' vulnerability values are estimated using verbal categories and assigning points to these categories.

Since vulnerability varies in different scenarios, not every field needs to contain an entry. Therefore, category 0 was introduced, which allows one to discard the combination concerned. The remaining categories are the same ones used to assess the likelihood of occurrence.

| Categories | Verbal categories | Description | Points |
|---|---|---|---|
| 0 | not relevant | The scenario is not relevant for the risk element. | 0 |
| 1 | very low | The vulnerability of the sub-process is very low. Hence, the scenario does not affect operations. | 1 |
| 2 | low | The vulnerability of the sub-process is low. Hence, the scenario requires organizational efforts (exchange of staff, repair, etc.) | 2 |
| 3 | medium | The vulnerability of the sub-process is medium. Hence, the scenario causes a partial, short-term disruption of operations. | 3 |
| 4 | high | The vulnerability of the sub-process is high. Hence, the scenario causes a partial, long-term disruption of operations. | 4 |
| 5 | very high | The vulnerability of the sub-process is very high. Hence, the scenario causes a complete, long-term disruption of operations. | 5 |

Table 5: Vulnerability categories

Now the vulnerability of each risk element and vulnerability criterion is assessed in the risk table. The points – V1 to V5[71] – are entered in the corresponding cells.

This is repeated for all risk elements. This results in a risk table which shows sub-vulnerabilities and sub-risks for the selected sub-process as well as the overall vulnerability and overall risk.

### V.4 Risk calculation

The connection, i.e. calculation of the values, is established using the described risk table as follows:

Points entered in the table:

| | |
|---|---|
| LO: | Likelihood of occurrence |
| DRE: | Dependence on risk elements |
| V1: | Dependence on external infrastructures – power supply |
| V2: | Dependence on external infrastructures – traffic, transport and logistics |
| V3: | Robustness/actual level of protection |
| V4: | Redundancy, substitutes |
| V5: | Restoration effort |

Values relating to risk elements calculated in the table:

| | |
|---|---|
| Sub-vulnerability | = DRE * (V1 + V2 + V3 + V4 + V5) |
| Sub-risk | = LO * DRE * (V1+V2+V3+V4+V5) |

Values relating to processes calculated in the table:

| | |
|---|---|
| Overall vulnerability | = sum of all sub-vulnerabilities |
| Overall risk | = sum of all sub-risks |

[71] Cf. tables 6 and 7.

| Sub-process: | Control room | Criteria of control room vulnerability | | | | | | Calculation | |
|---|---|---|---|---|---|---|---|---|---|
| Scenario: | Failure of external power supply | Dependence on risk elements | Dependence on external infrastructures – power supply | Dependence on external infrastructures – traffic, transport and logistics | Robustness/ actual level of protection | Redundancy, substitutes | Recovery effort | Sub-vulnera-bility | Sub-risk |
| LO: | 3 | | | | | | | | |
| Personal | Question | To what extent does the control room depend on special-ized staff? | How vulnerable is the control room due to the staff's dependence on external power supply? | How vulnerable is the control room due to the staff's depend-ence on traffic, transport and logistics? | How vulnerable is the control room due to a lack of physical protection for staff? | How vulnerable is the control room due to the lack of substitute staff in case of a blackout? | How vulner-able is the sub-process with regard to the time needed to reassign staff? | | |
| | Comments | The control room is very dependent on staff. | Staff are dependent on power supply only to a lim-ited extent. For example, the lack of emergen-cy lighting may impair work. | External power supply may affect traffic and transport. Staff may not be able to reach the workplace. | Lack of emer-gency lighting may cause accidents and injuries. | The blackout will have only a low or medium impact on the availability of substitute staff (impairment of public transpor-tation, rail traffic). | After the black-out, staff will no longer be affected. | | |
| | Points | 5 | 1 | 3 | 1 | 2 | 1 | 40 | 120 |

Table 6: Extract from the risk table for the control room

The following table shows a sample result for all risk elements of the control room. In this table, all questions and comments were deleted for the sake of clarity. Facilities and equipment are summarized under “Facilities and Equipment”.

| Sub-process: | Control room | Criteria of control room vulnerability | | | | | | Calculation | |
|---|---|---|---|---|---|---|---|---|---|
| Scenario: | Failure of external power supply | Dependence on risk elements | Dependence on external infrastructures – power supply | Dependence on external infrastructures – traffic, transport, logistics | Robustness/actual level of protection | Redundancy, substitutes | Recovery effort | Sub-vulnerability | Sub-risk |
| LO: | 3 | | | | | | | | |
| Staff | Points | 5 | 1 | 3 | 1 | 2 | 1 | 40 | 120 |
| Premises, buildings | Points | 5 | 0 | 0 | 0 | 3 | 0 | 15 | 45 |
| Facilities, equipment | Points | 5 | 5 | 0 | 3 | 1 | 2 | 55 | 165 |
| Data, software | Points | 5 | 5 | 1 | 4 | 5 | 3 | 90 | 270 |
| Files | Points | 2 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| Raw and working materials | Points | 5 | 2 | 2 | 0 | 4 | 0 | 40 | 120 |
| Overall vulnerability, overall risk (sub-process, scenario): | | | | | | | | 240 | 720 |

Table 7: Risk table for the control room without questions or comments

### V.5 Risk comparison

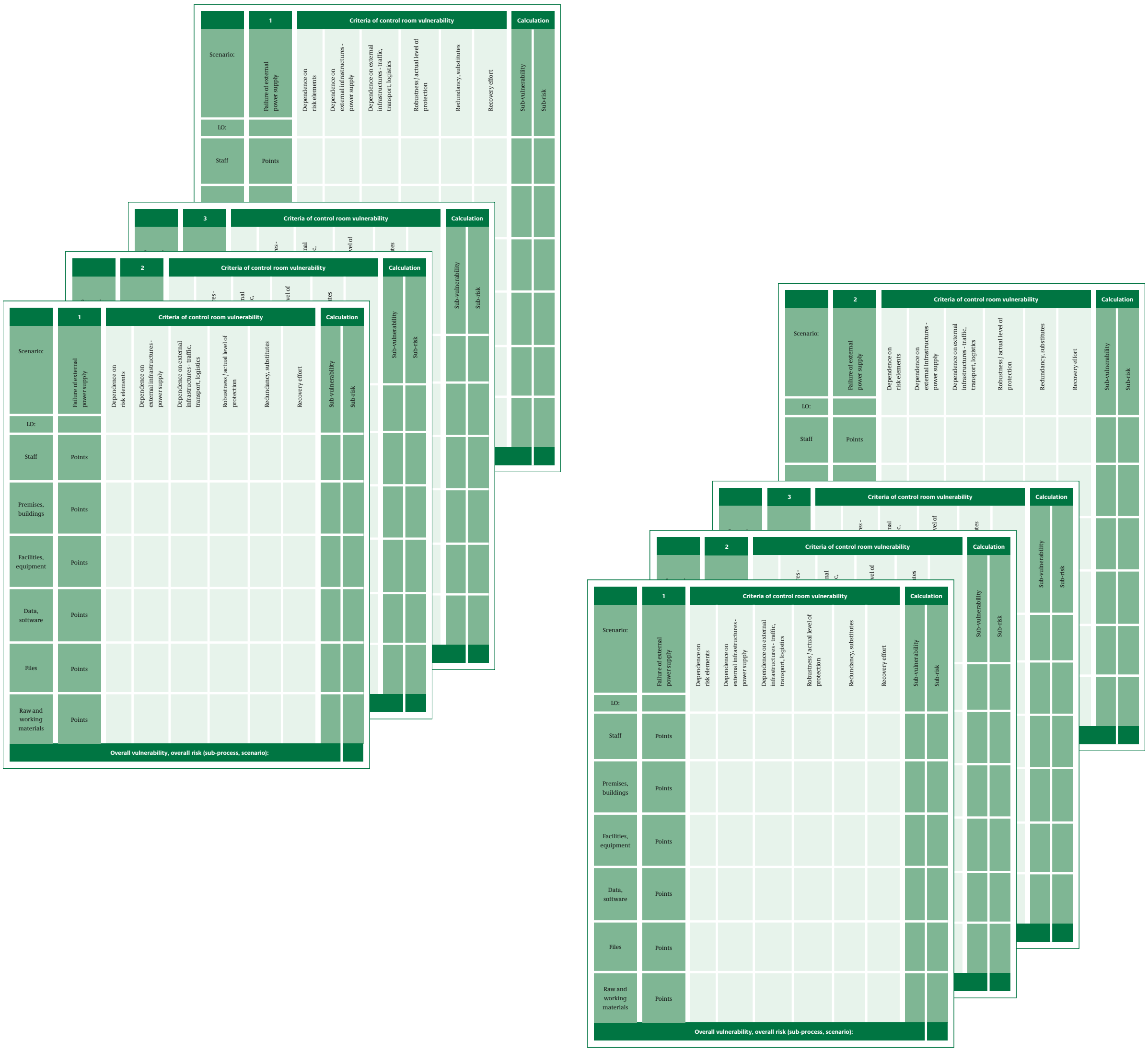
Using the results obtained from the analysis of all critical processes and their sub-processes in the facility and of the different scenarios relevant for the facility, risk tables can be created and compared. Results are generated on the same standardized, methodological and conceptual basis. Thus, the following aspects can be compared:

- sub-vulnerabilities and sub-risks of risk elements within the sub-process;
- sub-vulnerabilities and sub-risks of the same risk elements in different sub-processes;
- sub-vulnerabilities and sub-risks in different sub-processes;
- overall vulnerabilities and overall risks in different sub-processes.

In the example, only sub-vulnerabilities and sub-risks of the control room were compared. Applying this method to other sub-processes would result in a comprehensive comparison within the whole facility.

The following figure shows a schematic comparison of two sub-processes and different scenarios.

**Figure 12: Two sub-processes, several scenarios**


1
3
2
1
Criteria of control room vulnerability
Calculation
Scenario:
Failure of external power supply
Dependence on risk elements
Dependence on external infrastructures - power supply
Dependence on external infrastructures - traffic, transport, logistics
Robustness / actual level of protection
Redundancy, substitutes
Recovery effort
Sub-vulnerability
Sub-risk
LO:
Staff
Premises, buildings
Facilities, equipment
Data, software
Files
Raw and working materials
Points
Overall vulnerability, overall risk (sub-process, scenario):
2
3
2
1

The calculated sub-vulnerabilities and sub-risks can be assigned to verbal categories. In the categorization below, a value is assigned to a higher category if it exceeds the maximum value of the category concerned by one point.

The following results were obtained for the risk element "Data, Software". The sub-vulnerability is very high (90 points) and the sub-risk is high (270 points).[72]

| Sub-vulnerability | |
|---|---|
| **Points** | **Verbal categories** |
| 0 | no sub-vulnerability |
| 1 to 5 | very low sub-vulnerability |
| 6 to 20 | low sub-vulnerability |
| 21 to 45 | medium sub-vulnerability |
| 46 to 80 | high sub-vulnerability |
| 81 to 125 | very high sub-vulnerability |

Table 8: Categorization of the calculated sub-vulnerabilities

| Sub-risks | | |
|---|---|---|
| **Categories** | **Points** | **Verbal categories** |
| 0 | 0 | no sub-risk |
| 1 | 1 to 5 | very low sub-risk |
| 2 | 6 to 40 | low sub-risk |
| 3 | 41 to 135 | medium sub-risk |
| 4 | 136 to 320 | high sub-risk |
| 5 | 321 to 625 | very high sub-risk |

Table 9: Categorization of the calculated sub-risks

The overall vulnerability and overall risk of the sub-process "control room" can also be categorized in this way. The overall vulnerability (240 points) and the overall risk (720 points) are in the medium category.

| Overall vulnerability | |
|---|---|
| **Points** | **Verbal categories** |
| 0 | no overall vulnerability |
| 1 to 35 | very low overall vulnerability |
| 36 to 140 | low overall vulnerability |
| 141 to 315 | medium overall vulnerability |
| 316 to 560 | high overall vulnerability |
| 561 to 875 | very high overall vulnerability |

Table 10: Categorization of the calculated overall vulnerabilities

| Overall risks | | |
|---|---|---|
| **Categories** | **Points** | **Verbal categories** |
| 0 | 0 | no overall risk |
| 1 | 1 to 35 | very low overall risk |
| 2 | 36 to 280 | low overall risk |
| 3 | 281 to 945 | medium overall risk |
| 4 | 946 to 2240 | high overall risk |
| 5 | 2241 to 4375 | very high overall risk |

Table 11: Categorization of the calculated overall risks

[72] Cf. Chapter VI. 4. Risk calculation, Table 7.

The control room has a medium overall vulnerability and a medium overall risk. However, the risk element “Data and Software” has a very high sub-vulnerability and a high sub-risk. Facilities and equipment have the second highest sub-risk. This sub-risk can also be classified as high. If, in reality, further security measures were planned, they should be implemented for the two risk elements mentioned above.

**IMPORTANT NOTE:**
The comparison of risks should focus on sub-risks. High sub-risks make a sub-process very vulnerable and must therefore be reduced.

A high overall vulnerability or a high overall risk of a sub-process may indicate that there are several high sub-risks. In this case, considerable efforts need to be made to reduce the risks. But overall risks consisting exclusively of medium sub-risks are less relevant.

Instead of comparing printed risk tables, the calculated values such as sub-vulnerabilities and sub-risks may also be entered in a new table.

In this way, all results may be compiled on one sheet. This also allows for an easy graphical evaluation using the chart function of the spreadsheet programme.

**Published by**
Federal Ministry of the Interior
Alt-Moabit 101 D
10559 Berlin, Germany
www.bmi.bund.de

**Edited by**
Federal Office for Civil Protection and Disaster Assistance
Division II Emergency preparedness; Critical Infrastructures

**English translation by**
Translation Service of the Federal Ministry of the Interior

**Design**
MEDIA CONSULTA Deutschland GmbH,
Anita Drbohlav (design),
Petra Grampe, Helmut Spörl (editing),
René Hanhardt (production)

**Photo credits**
Federal Office of Civil Protection and Disaster Assistance (BBK)
Federal Agency for Technical Relief (THW)

**Printed by**
Bonifatius GmbH, Paderborn

**This brochure may be ordered free of charge from:**
Publikationsversand der Bundesregierung
Postfach 48 10 09
18132 Rostock, Germany
Phone: +49 18 05-77 80 90
(within Germany landline rate 14 cents/min; calls from mobile phones may be charged at a higher rate; as at Sept. 2007)
Fax: +49 18 05-77 80 94
(within Germany landline rate 14 cents/min; calls from mobile phones may be charged at a higher rate; as at Sept. 2007)
E-mail: publikationen@bundesregierung.de
Item no.: BMI08316

Any personal data required for mailing will be destroyed after the publication has been sent.

This brochure has been published free of charge as part of the public information work of the Federal Ministry of the Interior. It may not be used by any political party, candidate or campaign workers during an election campaign for purposes of campaign advertising. This applies to elections at the European, federal, state and local levels. In particular, distributing this publication at campaign events or at information stands of political parties, or inserting, stamping or attaching to it any political information or advertising constitutes misuse. Nor may it be passed on to third parties for purposes of campaign advertising. Regardless of when, by what means and in what quantities this publication was delivered to the recipient, even without reference to any upcoming election it may not be used in a manner that could be construed as bias by the Federal Government on behalf of any individual political group.